Multiemployer IT Summit

What's NExT?

Opening Address

Frank Tanz, VP and Senior Consultant, Segal's Administration & Technology Consulting Practice

Dave Wilsey, Director of Information Technology, UMWA Health and Retirement Funds

October 10-11, 2023 / San Diego

Proudly sponsored by

Segal

Agenda

1. Welcome
2. Steering Committee Introductions
3. Mobile App
4. 2022 IT Summit Survey Results
5. 2023 IT Summit Highlights
6. Future Topics

Steering Committee Introductions 2022 Committee

Name	Organization	Title
Barry Buckalew	National Elevator Industry Benefit Plans	Director, Information Technology
Randi Farber	Building Service 32BJ Benefit Funds	Director, Technology & Operations
Antonio Quinones	Carpenters Southwest Administrative Corporation	Director of Operations
Nafeeza S. Ramlochan	United Association National Pension Fund	Director of Operations & Organizational Development
Gokul Sheshadri	SAG AFTRA Plans	COO
Dave Wilsey	UMWA Health and Retirement Funds	Director of Information Technology
Alex Borucki	Segal	Consultant
Gisela de San Roman	Segal	Senior Consultant
Stuart Lerner	Segal	SVP and Practice Leader
Jesse Rivera	Segal	VP and Senior Consultant
Susan Schwarzman	Segal	Senior Consultant
Michael Stoyanovich	Segal	VP and Senior Consultant
Frank Tanz	Segal	VP and Senior Consultant

Steering Committee Introductions
Travel, Administrative and Marketing Support

Name	Organization	Title
Becky Herring	Segal	Associate Consultant
Brett McCarty	Segal	SVP, Marketing Leader
Tracie Saunders	Segal	Director, Business Operations
Jason Spears	Segal	Director Marketing
Agata Zak	Segal	Associate Consultant

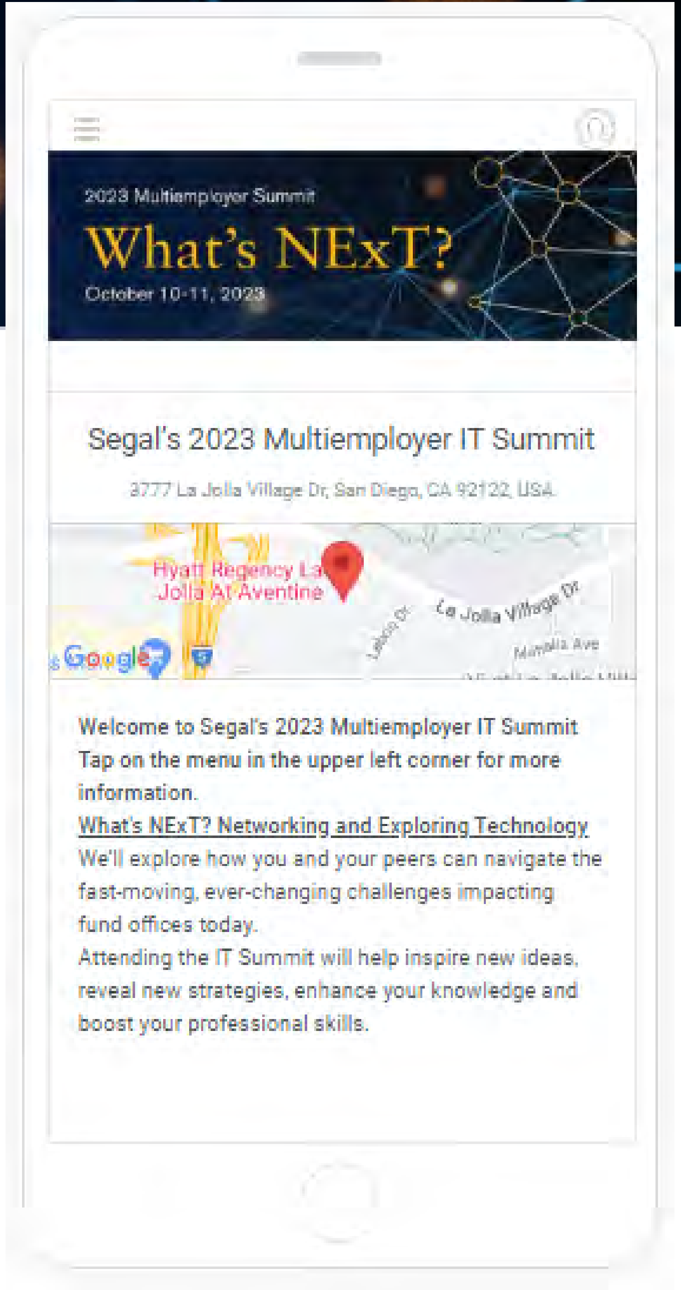
Logistics Overview

Tracie Saunders

- Breaks
- Breakfast
- Lunches
- Networking Dinner Event
- Raffle
- Other

Mobile App

- **Step 1** - Download the Guidebook app to your device
- **Step 2** - Open the Guidebook app
- **Step 3** - Enter the passphrase for Segal’s 2022 Multiemployer IT Summit.
  - The passphrase is: **mes2023**
- **Step 4** (Optional) - Sign in using your existing account



2023 Multiemployer Summit

What’s NExT?

October 10-11, 2023

Segal’s 2023 Multiemployer IT Summit

3777 La Jolla Village Dr, San Diego, CA 92122, USA

Welcome to Segal’s 2023 Multiemployer IT Summit
Tap on the menu in the upper left corner for more information.

What’s NExT? Networking and Exploring Technology

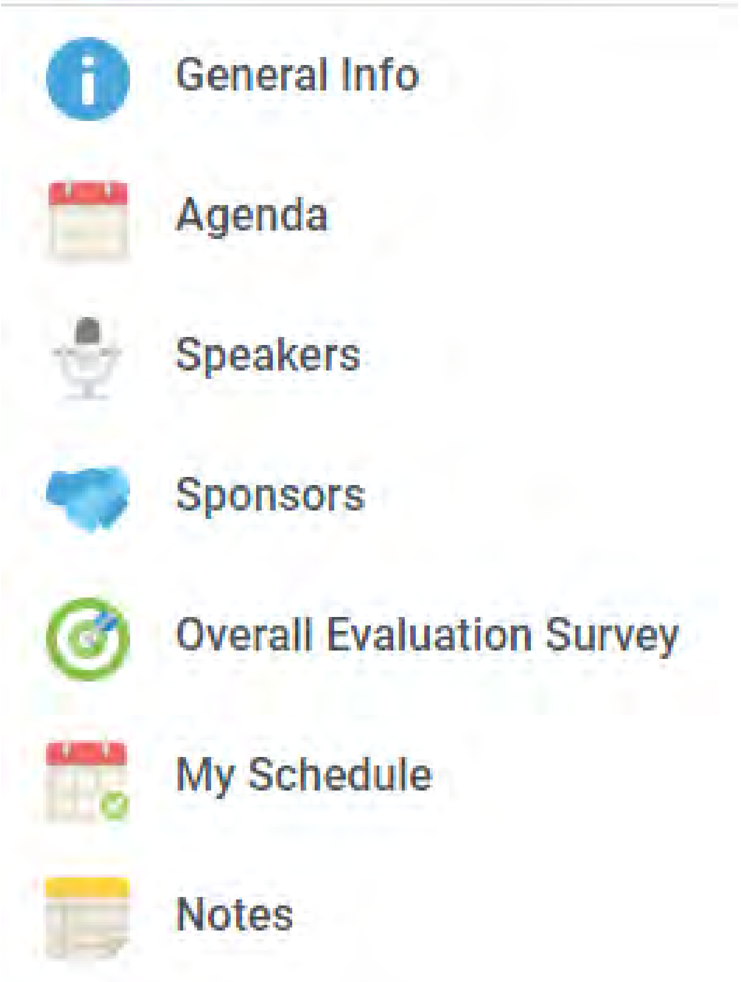
We’ll explore how you and your peers can navigate the fast-moving, ever-changing challenges impacting fund offices today.

Attending the IT Summit will help inspire new ideas, reveal new strategies, enhance your knowledge and boost your professional skills.

Mobile App Continued

Things you can do using the Mobile App:

- View the Agenda
- View Speaker Information
- View Sponsor Information
- Complete Surveys (Sessions and Overall)
- View Places of Interest
- Take Notes
- Create a Customized Schedule



General Info

Agenda

Speakers

Sponsors

Overall Evaluation Survey

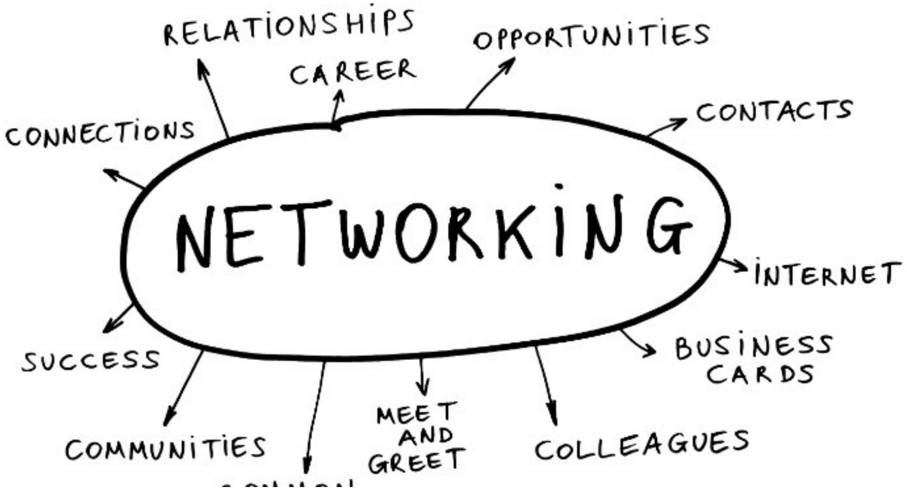
My Schedule

Notes

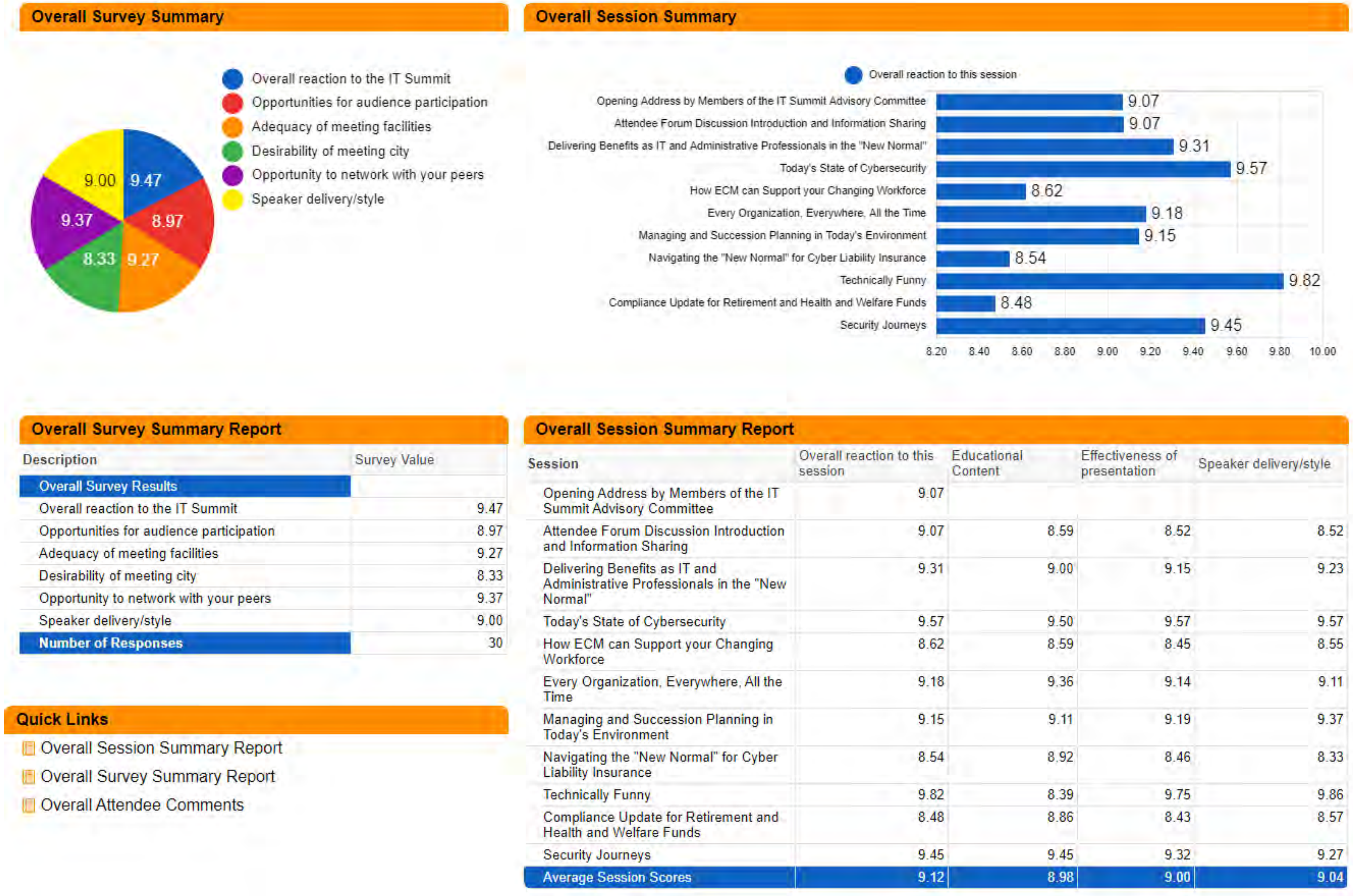
Let’s Take 5 Minutes

Networking Workshop

Challenge: Introduce Yourself to 3 People That You Don’t Know



2023 Multiemployer IT Summit Survey Results Overall Evaluation of the IT Summit



Overall Survey Summary

9.00
9.47
9.37
8.97
8.33
9.27
● Overall reaction to the IT Summit
● Opportunities for audience participation
● Adequacy of meeting facilities
● Desirability of meeting city
● Opportunity to network with your peers
● Speaker delivery/style

Overall Session Summary

● Overall reaction to this session
Opening Address by Members of the IT Summit Advisory Committee
9.07
Attendee Forum Discussion Introduction and Information Sharing
9.07
Delivering Benefits as IT and Administrative Professionals in the "New Normal"
9.31
Today's State of Cybersecurity
9.57
How ECM can Support your Changing Workforce
8.62
Every Organization, Everywhere, All the Time
9.18
Managing and Succession Planning in Today's Environment
9.15
Navigating the "New Normal" for Cyber Liability Insurance
8.54
Technically Funny
9.82
Compliance Update for Retirement and Health and Welfare Funds
8.48
Security Journeys
9.45
8.20
8.40
8.60
8.80
9.00
9.20
9.40
9.60
9.80
10.00

Overall Survey Summary Report

Description	Survey Value
Overall Survey Results	
Overall reaction to the IT Summit	9.47
Opportunities for audience participation	8.97
Adequacy of meeting facilities	9.27
Desirability of meeting city	8.33
Opportunity to network with your peers	9.37
Speaker delivery/style	9.00
Number of Responses	30

Quick Links

- Overall Session Summary Report
- Overall Survey Summary Report
- Overall Attendee Comments

Overall Session Summary Report

Session	Overall reaction to this session	Educational Content	Effectiveness of presentation	Speaker delivery/style
Opening Address by Members of the IT Summit Advisory Committee	9.07			
Attendee Forum Discussion Introduction and Information Sharing	9.07	8.59	8.52	8.52
Delivering Benefits as IT and Administrative Professionals in the "New Normal"	9.31	9.00	9.15	9.23
Today's State of Cybersecurity	9.57	9.50	9.57	9.57
How ECM can Support your Changing Workforce	8.62	8.59	8.45	8.55
Every Organization, Everywhere, All the Time	9.18	9.36	9.14	9.11
Managing and Succession Planning in Today's Environment	9.15	9.11	9.19	9.37
Navigating the "New Normal" for Cyber Liability Insurance	8.54	8.92	8.46	8.33
Technically Funny	9.82	8.39	9.75	9.86
Compliance Update for Retirement and Health and Welfare Funds	8.48	8.86	8.43	8.57
Security Journeys	9.45	9.45	9.32	9.27
Average Session Scores	9.12	8.98	9.00	9.04

2023 Multiemployer IT Summit Highlights

Networking Opportunities		
Session/Event	**Day/Time**	**Presenter(s)/Comments**
Opening Address by Members of the IT Summit Advisory Committee	8:30am – 9:00am **Today**	Frank Tanz, Dave Wilsey
Attendee Forum Discussion Introduction and Information Sharing	9:00am – 11:00am **Today**	Barry Buckalew, Stuart Lerner
Networking Lunch	1:00pm – 2:00pm **Today**	
Networking Dinner	6:00pm – 9:00pm **Tonight**	George’s at the Cove (1250 Prospect Street, La Jolla, CA 92037)
Networking Lunch and Raffle	12:00pm – 1:00pm **Tomorrow**	

2023 Multiemployer IT Summit Highlights

Administration /Technology Sessions

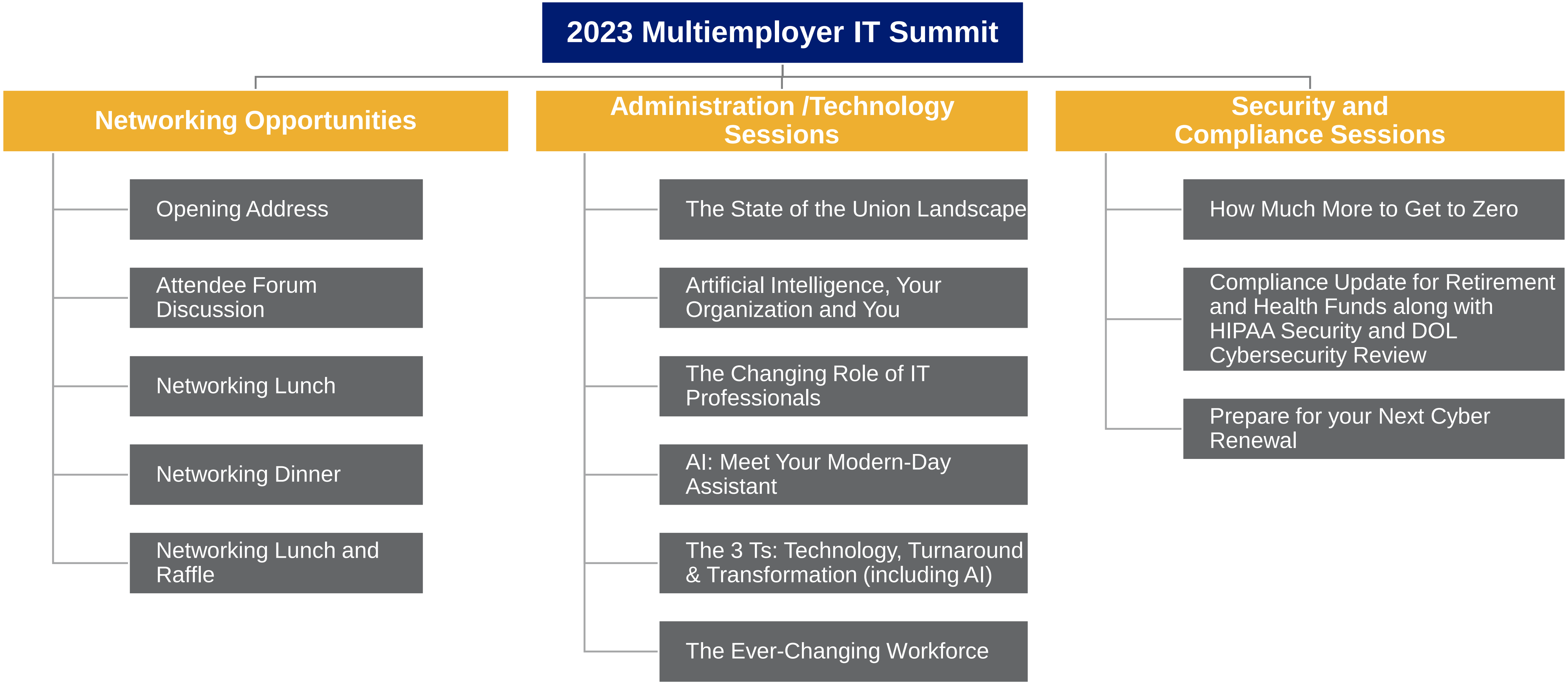
Session/Event	Day/Time	Presenter(s)/Comments
The State of the Union Landscape	11:15am –12:00pm **Today**	David Brenner
Artificial Intelligence, Your Organization and You	12:00pm – 1:00pm **Today**	Randi Farber, Gokul Sheshadri, Michael Stoyanovich
The Changing Role of IT Professionals	3:15pm – 4:15pm **Today**	William Feyling, Kyle Hughes, Arturo Miramontes, Antonio Quinones, Jesse Rivera, Susan Schwarzman, Dave Wilsey
AI: Meet Your Modern-Day Assistant	8:00am – 9:00am **Tomorrow**	Christina "CK" Kerley / Keynote
The 3 Ts: Technology, Turnaround & Transformation (including AI)	11:00am – 12:00pm **Tomorrow**	Joel Manfredo
The Ever-Changing Workforce	1:00pm – 2:00pm **Tomorrow**	Alex Borucki, Daniel Beaman, Michael Donovan, Jon Melander, Steve Ostrander, Susan Paul, Amy S. Timmons

2023 Multiemployer IT Summit Highlights

Security and Compliance Sessions

Session/Event	Day/Time	Presenter(s)/Comments
How Much More to Get to Zero	2:00pm – 3:00pm **Today**	Cameron Matthews
Compliance Update for Retirement and Health Funds along with HIPAA Security and DOL Cybersecurity Review	9:15am – 10:45am **Tomorrow**	Michael Stoyanovich, Kristina M. Zinnen
Prepare for your Next Cyber Renewal	2:00pm – 3:00pm **Tomorrow**	Matthew Jackson, Scott Schreiber

2023 Multiemployer IT Summit Highlights Summary



2023 Multiemployer IT Summit

Networking Opportunities

- Opening Address
- Attendee Forum Discussion
- Networking Lunch
- Networking Dinner
- Networking Lunch and Raffle

Administration /Technology Sessions

- The State of the Union Landscape
- Artificial Intelligence, Your Organization and You
- The Changing Role of IT Professionals
- AI: Meet Your Modern-Day Assistant
- The 3 Ts: Technology, Turnaround & Transformation (including AI)
- The Ever-Changing Workforce

Security and Compliance Sessions

- How Much More to Get to Zero
- Compliance Update for Retirement and Health Funds along with HIPAA Security and DOL Cybersecurity Review
- Prepare for your Next Cyber Renewal

Future Topics

- Your Participation and Contribution to the Conference is Appreciated and Welcome.
- Please Speak up During the Sessions and Networking Events and Communicate Topics of Interest that Might Benefit the Group.

Thank You

**For more info,
please contact us**

Frank Tanz

fetanz@segalco.com
484.410.7431

Dave Wilsey

Dwilsey@umwafunds.org
202.521.2264

Multiemployer IT Summit

What’s NExT?

Attendee Forum Discussion Introduction and Information Sharing

Barry Buckalew, Director of Information Technology,
National Elevator Industry Benefit Plans

Stuart Lerner, SVP and Practice Leader,
Segal’s Administration & Technology Consulting Practice

October 10-11, 2023 / San Diego

Proudly sponsored by

Segal

Agenda

1. Segal and Fund Office Introductions
2. TPA & Other Professional Organization Introductions
3. Sponsor Introductions

Segal and Fund Office Introductions

Segal's Administration & Technology Consulting Practice

Presenter: Stuart Lerner, SVP and Practice Leader

Other Attendees: Alex Borucki, Consultant; Jesse Rivera, VP and Senior Consultant; Susan Schwarzman, Senior Consultant; Michael Stoyanovich, VP and Senior Consultant; Frank Tanz, VP and Senior Consultant; Amy S. Timmons, SVP and Senior Consultant

Segal

National Elevator Industry Benefit Plans

Presenter: Barry Buckalew, Director of IT

Other Attendees: Diana Mosier, Software Support & Development Manager; Joe Puckett, Network and Telecommunications Manager

Top three initiatives:

- Migration of majority of on-prem servers to Azure- Including moving to O365, Citrix Cloud Data Center 2.0 - Moving virtually all on-premise presence to Azure
- Implementation of Mobile Device Management System
- NSA/Transparency in Coverage Pricing Tool

Benefits administration system:

- Bridgeway/basys

Enterprise Content Management System (ECM):

- OnBase

Phone system:

- Avaya

Bakery and Confectionery Health

Presenter: John Harrison, IT Department Manager

Other Attendees: Caleb Horton, Systems Engineer

Top three initiatives:

- Migration to Basys Hosted System
- Integration of Zelis for Check Printing
- Building Maintenance/Repairs and/or Relocation

Benefits administration system:

- In-House Legacy Mainframe

Enterprise Content Management System (ECM):

- OnBase (once on Basys)

Phone system:

- E-MetroTel / VOip.MS

Building Service 32BJ Benefit Funds

Presenter: Randi Farber, Director, Technology & Operations

Other Attendees: N/A

Top three initiatives:

- Implementation of an upgraded benefit administration system
- HIPAA Risk Assessment
- VDI

Benefits administration system:

- Vitech

Enterprise Content Management System (ECM):

- SharePoint

Phone system:

- Cisco Call Manager

Carpenter Funds Administration Office of Northern California

Presenter: Alan Larson, Director of Information Technology

Other Attendees: Bill Feyling, Administrator; Russ Fairles, Director of Regulations and Internal Affairs; Jason Price, Manager of Support and Systems Services

Top three initiatives:

- Implement and Expand New Benefits Admin System
- Migrate Core Services to the Cloud
- Enhance Self Service Options

Benefits administration system:

- Vitech

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Avaya

Carpenters Combined Funds

Presenter: Mike Swiderski, Controller

Other Attendees: N/A

Top three initiatives:

- Implementation of a new benefits administration system (FACTs to ISSI)
- HIPAA Risk Assessment
- Automation

Benefits administration system:

- ISSI (Beginning Oct 15)

Enterprise Content Management System (ECM):

- DocuWare

Phone system:

- Avaya

Carpenters Southwest Administrative Corporation

Presenter: Antonio Quinones, Director of Operations

Other Attendees: Anthony Nickell, IT Operations Manager

Top three initiatives:

- Cybersecurity
- Self-service tools
- Digitizing the Fund

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- Hyland OnBase

Phone system:

- 8x8

CCPOA Benefit Trust Fund

Presenter: Peter Sands, IT Supervisor

Other Attendees: Daniel Beaman, Administrator; James Baumiller, Assistant Administrator; Jordan Bargas, I.T. Computer Operator and Data Research Technician

Top three initiatives:

- EDI / Auto Adjudication
- Paperless / ECM
- Payments with Zelis

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- N/A

Phone system:

- RingCentral

Central Laborers Pension Fund

Presenter: Kyle Forshee, Business Analyst, IT

Other Attendees: N/A

Top three initiatives:

- DOL Cyber Security Audit
- Business Intelligence Target State
- Workflow Efficiency and Automation

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- Onbase

Phone system:

- Mitel

Central Pension Fund of the International Union of Operating Engineers and Participating Employers

Presenter: Greg Drauch, COO

Other Attendees: Susheal Gupta, IMS Manager

Top three initiatives:

- Start implementing new pension administration system
- Enhance security program
- Operations review

Benefits administration system:

- Custom

Enterprise Content Management System (ECM):

- Perceptive Content

Phone system:

- RingCentral

Chicago & Vicinity Laborers District Council Funds

Presenter: Rini Torano, Director of IT

Other Attendees: Yelena Meltser, Senior Developer

Top three initiatives:

- Implementation of SIEM
- IT Audit
- Disaster Recovery Plan

Benefits administration system:

- Vitech

Enterprise Content Management System (ECM):

- FIS EXP

Phone system:

- Mitel

Directors Guild of America – Producer Pension and Health Plans

Presenter: Peter Melika, CTO / CSO

Other Attendees: N/A

Top three initiatives:

- Risk & Compliance Assessments
- Staffing
- Cyber Security

Benefits administration system:

- V3

Enterprise Content Management System (ECM):

- Laserfiche

Phone system:

- Cisco

IAM National Pension Fund

Presenter: Ronald Novak, Director, Information Technology

Other Attendees: N/A

Top three initiatives:

- Implementation of New Benefit Administration System for Benefit Trust Fund
- Security Audit 4Q23
- HIPAA Risk Assessment and Security Audit 4Q24

Benefits administration system:

- Vitech

Enterprise Content Management System (ECM):

- V3 internal ECM and RingCentral Phone System

Phone system:

- RingCentral

IBEW Local 103 Trust Funds

Presenter: **Michael P. Donovan, Administrator**

Other Attendees: N/A

Top three initiatives:

- HIPAA Risk Assessment
- vCISO Implementation
- SharePoint Migration

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Avaya

Ironworkers Mid America Pension and SMA

Presenter: Joseph Paul Burke, IT Coordinator

Other Attendees: N/A

Top three initiatives:

- New version of database software
- Adding security functionality for office employees
- Moving to cloud services for backups

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Zultys

IUOE Local 15

Presenter: **Vincent Turano, IT Administrator**

Other Attendees: Yasir Eltayeb, Database Administrator

Top three initiatives:

- Cloud Phone System
- New Benefits/Document System
- SharePoint

Benefits administration system:

- Vitech

Enterprise Content Management System (ECM):

- In-House Programming

Phone system:

- SmartChoice Communications

IBEW Local 369

Presenter: Emilie Hall, Office Manager

Other Attendees: N/A

Top three initiatives:

- Multifactor Authentication
- Staffing
- Increasing Self Service

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- N/A

Phone system:

- N/A

Laborers Funds Administrative Office of Northern California, Inc.

Presenter: Kyle Hughes, Director of Information Technology

Other Attendees: Alex Vega, Information Technology Manager

Top three initiatives:

- Phone System Replacement
- Cloud Compute Tenant Buildout
- Migrating off of Atlassian Products

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- OnBase / FIS EXP

Phone system:

- Avaya

Local 11 Ironworkers Benefit Funds

Presenter: Andrew Roos, IT Manager

Other Attendees: N/A

Top three initiatives:

- Annual Cyber Security Awareness Training
- Security and Risk Assessment
- File Service Migration to Egnyte

Benefits administration system:

- Basys\Bridgeway

Enterprise Content Management System (ECM):

- OnBase

Phone system:

- GoTo

Maters, Mates & Pilots Health and Benefit Fund

Presenter: **Michael McCullough, Director of IT and Operations**

Other Attendees: N/A

Top three initiatives:

- Member/Provider Portal
- Cyber Security
- Workflows/process and procedures.

Benefits administration system:

- In house

Enterprise Content Management System (ECM):

- Sharepoint

Phone system:

- Avaya

Mesa Public Schools

Presenter: David Sanders, Chief Technology Officer

Other Attendees: Romeo Vega, Systems Security Analyst

Top three initiatives:

- Cybersecurity user awareness and training
- System and organization efficiency
- Security Ops Center (Managed)

Benefits administration system:

- BenefitFocus

Enterprise Content Management System (ECM):

- Tyler Visions

Phone system:

- Cisco VoIP

Motion Picture Industry Pension & Health Plans

Presenter: **Joel Manfredo, Chief Information, Innovation & Digital Officer**

Other Attendees: **Michael Rich, Director, Security I&O**

Top three initiatives:

- Automation
- Website/Mobile App Redux
- Enterprise Content Management

Benefits administration system:

- Vitech, Sagitec, QNXT

Enterprise Content Management System (ECM):

- To be replaced

Phone system:

- ATT

Operating Engineers Funds, Inc.

Presenter: **Juan Pablo Yah Yah, Director, IT Security and Infrastructure**

Other Attendees: N/A

Top three initiatives:

- Cybersecurity
- Merge services under few tools
- Increase self-service

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- N/A

Phone system:

- N/A

New England Healthcare Employees Welfare and Pension Fund

Presenter: **Silvana Stankus, Executive Director**

Other Attendees: N/A

Top three initiatives:

- RFP for review of benefits and potential change of carrier
- Claim System for welfare and pension upgrade
- Potential increase of self service

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Microsoft

Pipe Trades Services MN

Presenter: Patrick Doody, IT Manager

Other Attendees: Jonathan Melander, Administrator

Top three initiatives:

- Implementation of new benefits system (ISSI/Bridgeway)
- Fund Office Reorg
- Hiring and training of new staff

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- ImageSilo

Phone system:

- in house ipitomy system

Pipeline Industry Benefit Fund

Presenter: **Steve Rowden, Operations Manager**

Other Attendees: N/A

Top three initiatives:

- Migration of Pension and H&W application to the cloud
- HIPAA Risk Assessment
- Ongoing Cybersecurity training/awareness

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- ImageSilo

Phone system:

- ATT

RWDSU/UFCW Local 338

Presenter: Edward Cimafonte, IT Director

Other Attendees: Earl Mathurin, Funds Administrator

Top three initiatives:

- New Benefits/Union Administration System
- Cybersecurity Audit/Remediation
- Systems/Infrastructure Upgrades

Benefits administration system:

- CHS Novus

Enterprise Content Management System (ECM):

- Docuware

Phone system:

- NEC Univerge

SAG-AFTRA Health Plan/SAG Producers Pension Plan

Presenter: **Gokul Sheshadri, Chief Operating Officer**

Other Attendees: N/A

Top three initiatives:

- Contact Center Replacement
- Pension System Replacement
- Data Engineering & Analytics Maturity

Benefits administration system:

- Homegrown for Eligibility, Contributions and Pension. Vitech legacy system for Contact Center.

Enterprise Content Management System (ECM):

- OpenText

Phone system:

- Cisco

SCUFCW Unions & Food Employers Joint Benefit Funds Admin, LLC

Presenter: **Jeff Randall, Chief Information Officer**

Other Attendees: N/A

Top three initiatives:

- Microsoft 365 Cloud Migration
- Managed XDR SOC
- PC Desktop Refresh

Benefits administration system:

- Developed in-house

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Cisco Unified Communications

SEIU Benefit Funds

Presenter: **Donna Joseph-Munroe, IT Program Manager**

Other Attendees: N/A

Top three initiatives:

- Closeout of Benefit Systems Administration Project
- Implementation of MFA across external Portals
- Implementation and Support of Self Services Portals - Members and Employers

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- OnBase

Phone system:

- Cisco Finesse

SEIU Healthcare IL Benefit Funds

Presenter: **Jennifer Mack, Executive Analyst & Strategic Coordinator**

Other Attendees: N/A

Top three initiatives:

- Wrapping up Benefits Administration System Implementation and planning/prep for supplemental related initiatives (automations, etc)
- Cybersecurity Audit / Risk Assessment
- Succession Planning/Staffing/Re-Organization

Benefits administration system:

- basys/Bridgeway

Enterprise Content Management System (ECM):

- OnBase

Phone system:

- Five9

Sheet Metal Workers Local 73 Welfare Pension Fund

Presenter: **James Feinberg, Assistant Fund Administrator**

Other Attendees: N/A

Top three initiatives:

- Member Portal
- Staffing
- Move to SharePoint

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- Papervision

Phone system:

- Breeze

Sheet Metal Workers' National Pension Fund

Presenter: Richard Duvall, IT Director

Other Attendees: N/A

Top three initiatives:

- Implementation of a new benefits administration system
- DOL cybersecurity best practices
- Disaster Recovery

Benefits administration system:

- Basys

Enterprise Content Management System (ECM):

- OnBase

Phone system:

- Microsoft Teams

So Cal IBEW-NECA Administrative Corp

Presenter: Celso Perez, Technology Director

Other Attendees: N/A

Top three initiatives:

- Cybersecurity and business continuity
- multifactor authentication
- increasing self-service and business efficiency

Benefits administration system:

- Trust Partner by Trust Benefit Technologies

Enterprise Content Management System (ECM):

- SharePoint

Phone system:

- Mitel

Transit Employees' H&W Plan

Presenter: Stephanie Steven, Director of Special Projects

Other Attendees: N/A

Top three initiatives:

- N/A
- N/A
- N/A

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- N/A

Phone system:

- N/A

UA Local 13 Benefit Office

Presenter: **Steve Ostrander, Fund Administrator**

Other Attendees: N/A

Top three initiatives:

- goISSI Microsoft Azure Platform Transition
- Member Portal Enhancements
- Cyber Risk Assessments/ DOL Compliance & Exceeding Requirements

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- N/A

Phone system:

- N/A

UFCW & Employers Trust, LLC

Presenter: Ken Foulke, Senior IT Manager

Other Attendees: Chenna Kothur, IT Applications Manager; Vineel Cherukula, IT Applications Manager

Top three initiatives:

- Core Admin Upgrade of the Vitech V3 Benefits Management system
- Enhance 2024 Open Enrollment process via improvements to Enrollment module and real-time reporting
- Improve member communication and reduce mailing costs through expanded use of online Member Self Service portal and email notifications

Benefits administration system:

- Vitech V3locity

Enterprise Content Management System (ECM):

- Vitech

Phone system:

- Avaya

UFCW Local 880 Benefit Funds

Presenter: **David Everhart, System Administrator**

Other Attendees: John Halkias, Administrative Manager

Top three initiatives:

- Succession planning
- Website/ Member portal
- disaster recovery planning/testing

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Go To connect

UFCW National Health and Welfare Fund

Presenter: Brenda C. Garma, Associate Executive Director

Other Attendees: N/A

Top three initiatives:

- Increasing self service
- New Cloud PBX
- Cybersecurity enhancements

Benefits administration system:

- ISSI

Enterprise Content Management System (ECM):

- SharePoint

Phone system:

- Nextiva

UMWA Health and Retirement Funds

Presenter: **David Wilsey, Director of Information Technology**

Other Attendees: N/A

Top three initiatives:

- Select and implement a new Benefits Administration System
- Complete HIPAA and cybersecurity audit recommendations
- Update in-house developed legacy applications

Benefits administration system:

- In-house developed

Enterprise Content Management System (ECM):

- ApplicationXtender

Phone system:

- Cisco

United Association

Presenter: Jason Pope, Sr., Director of IT

Other Attendees: N/A

Top three initiatives:

- Application Development
- Security / Infrastructure Updates
- Policy Development / Implementation

Benefits administration system:

- Basys, ISSI

Enterprise Content Management System (ECM):

- N/A

Phone system:

- RingCentral

United Association National Pension Fund (UANPF)

Presenter: Tseday Yimer, Benefit Determination Supervisor

Other Attendees: Joseph Youhouse, Pension Department Assistant Manager; Venkat Kukkala, Project Lead - Software Development; David Johnson, Database Application Developer

Top three initiatives:

- Migration to goBasys hosted environment
- Upgrading ServiceXG Pension module including Fund-specific enhancements
- Research and implementation of cloud-based hosted backups and disaster recovery site

Benefits administration system:

- basys

Enterprise Content Management System (ECM):

- Onbase

Phone system:

- Avaya

TPA & Other Professional Organization Introductions

BeneSys, Inc.

Presenter: Jeff Spires, CIO

Other Attendees: Jay Roberts, Customer Success Manager; Don Herman, Director of Software Engineering

Top three initiatives:

- Azure Migration
- Retiring Old Systems
- Upgrading Member Facing Systems

Benefits administration system:

- BenefitDriven

Enterprise Content Management System (ECM):

- Hyland OnBase

Phone system:

- Mitel

Health Services & Benefit Administrators, Inc. (HS&BA)

Presenter: Arturo Miramontes, CEO|COO

Other Attendees: N/A

Top three initiatives:

- Cybersecurity
- Succession planning and staffing
- Imaging and automation

Benefits administration system:

- Bridgeway (ISSI-Ultra)

Enterprise Content Management System (ECM):

- Perceptive Content and SharePoint

Phone system:

- Zoom Phone - CC

Wilson-McShane Corporation

Presenter: Zak Kotnik, CSO

Other Attendees: N/A

Top three initiatives:

- Third-party Assessment
- Cloud Migration
- Client Implementations

Benefits administration system:

- In-house, basys, and ISSI

Enterprise Content Management System (ECM):

- Onbase

Phone system:

- Mitel

Zenith American Solutions

Presenter: Susan Paul, Chief Operating Officer

Other Attendees: Roberto Hormazabal, Chief Client Relations & Business Development Officer

Top three initiatives:

- Customer Service Modernization
- Quality Center of Excellence
- Improving and Increase Self Service Tools and Capabilities

Benefits administration system:

- We use many systems.

Enterprise Content Management System (ECM):

- Sharepoint

Phone system:

- TCN

Weinberg, Roger & Rosenfeld

Presenter: **Zachary Daniel Angulo, Attorney**

Other Attendees: N/A

Top three initiatives:

- Cybersecurity Assessment
- Succession Planning
- Incident Response Planning

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- N/A

Phone system:

- N/A

Sponsor Introductions

Green Light

Presenter: **Matt Davis, CEO**

Other Attendees: Mark Winner, COO

Top three initiatives:

- Price Comparison Tool - Transitioning from 500 Items or Services to ALL Items or Services.
- Integration of Single-Sign On Across Member Facing Platforms
- Development of API Services for Electronic Cost Management Programs

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- N/A

Phone system:

- Internally Managed PBX - Yealin

Green Light Overview

Market Segment:
Technology-Enabled Services for Health Plans

Mission:
We exist to help health plan dollars go as far as possible.

Primary Focus Areas

Workflow & Process Automation

Cost Management Optimization

NSA / TiC Compliance

Key Differentiators

- Alignment With the Health Plans We Serve
- Knowledge Sharing With Health Plan Stakeholders
- NextGen Methodology Yields Unparalleled Results
- Overall Security Maturity – Current Certifications include:
  - HITRUST CSF r2
  - SOC2 Type 2

Contact Information

For more info, please contact us

Matt Davis, CEO
mdavis@greenlightcm.com

Mark Winner, COO
mwinner@greenlightcm.com

Premier Technology Solutions, Inc.

Presenter: Michael Golusinski, Vice President

Other Attendees: Scott Schreiber, Technical Project Manager

Top three initiatives:

- Office Move
- IaaS to SaaS migration
- New Security Tools evaluation

Benefits administration system:

- N/A

Enterprise Content Management System (ECM):

- SharePoint

Phone system:

- Microsoft Teams

About Premier

Microsoft Gold Partner with over 25 years of experience providing technology advice and assistance.

Security Partner for Segal Consulting helping to identify and remediate security issues.

Using Know-How gained to improve our client's technology.

Managed Service and Security for the multiemployer community.

What can we do for you?

Network/Cloud Security Assessment/Remediation

Cloud Migration Assistance

Managed Services and Managed Security Services

Staff Augmentation

Emergency Incident Response

Contact Information

**For more info,
please contact us**

mgolusinski@premiertechnolgoy.com
212-576-1602

Thank You

For more info, please contact us

bbuckalew@neibenefits.org
610-325-9100

slerner@segalco.com
212-251-5389

Multiemployer IT Summit

What’s NExT?

The State of the Union Landscape

David Brenner, SVP and National Director of Multiemployer Consulting

October 10-11, 2023 / San Diego

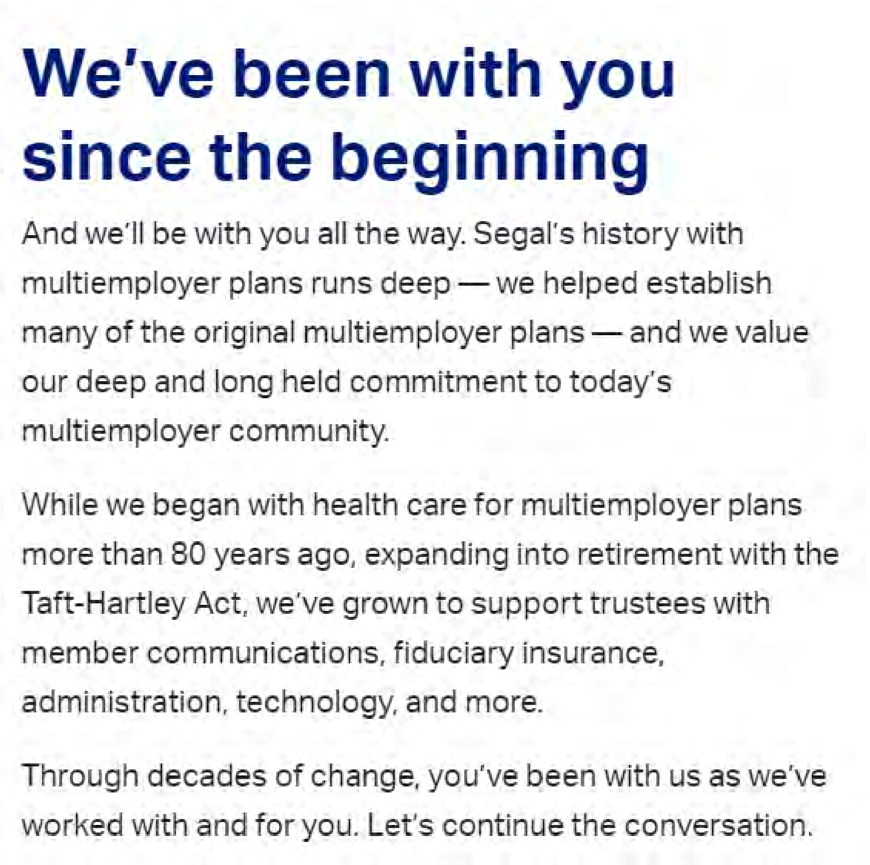
Proudly sponsored by

Segal

Agenda

- Segal Multiemployer
- Our Multiemployer Clients Include
- Number of Retirement Clients
- Number of Health Clients
- Organized labor in a Changing Economy
- Strikes and Negotiations

Segal Multiemployer



We've been with you since the beginning

And we'll be with you all the way. Segal's history with multiemployer plans runs deep — we helped establish many of the original multiemployer plans — and we value our deep and long held commitment to today's multiemployer community.

While we began with health care for multiemployer plans more than 80 years ago, expanding into retirement with the Taft-Hartley Act, we've grown to support trustees with member communications, fiduciary insurance, administration, technology, and more.

Through decades of change, you've been with us as we've worked with and for you. Let's continue the conversation.

We've been in the Multiemployer Market for more than 80 years.

Our Multiemployer Clients Include

- DB Retirement Trust Funds
- DC Retirement Trust Funds (Annuity Plans)
- Health & Welfare Trust Funds
- Apprenticeship and Training Funds
- 59 Unions and Contributing Employers and various services related to their collective bargaining

Number of Retirement Clients

Defined Benefit Plans

1,230
Active Taft-Hartley Plans

612
Segal DB Clients

370 Valuations

Construction	217
Entertainment	20
Manufacturing	25
Retail/Food	25
Service	26
Transportation	57

Defined Contribution Plans

1,038
Taft-Hartley Plans

575
Participant Directed 105
Taft-Hartley 401(K) Plans

463
Trustee Directed Plans

117*
Segal DC Clients

215
Segal Marco DC Clients

* Excluding SMA.

Number of Health Clients

Taft Hartley Health and Welfare Medical Plans in the US

Approx. 1,593

995

funds with
500 – 99,999
active participants
(households) averaging **3,693**

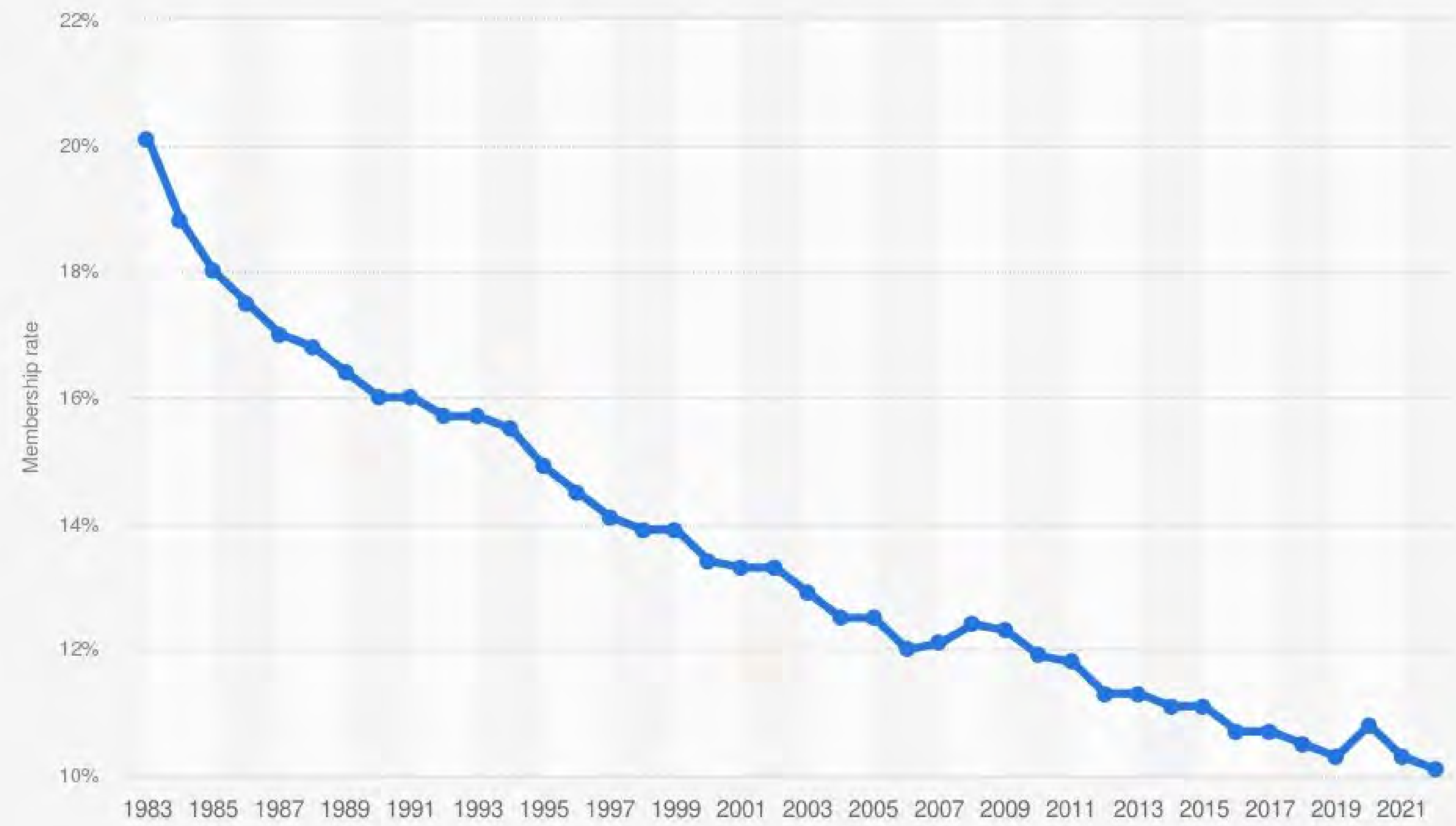
4

funds with
100,000 – 196,000
active participants
(households)

519

Segal H&W
Clients

Rate of union membership of employees in the United States from 1983 to 2022



Source
Bureau of Labor Statistics
© Statista 2023

Additional Information:
United States; 1983 to 2022; 16 years and older

Organized labor in a Changing Economy

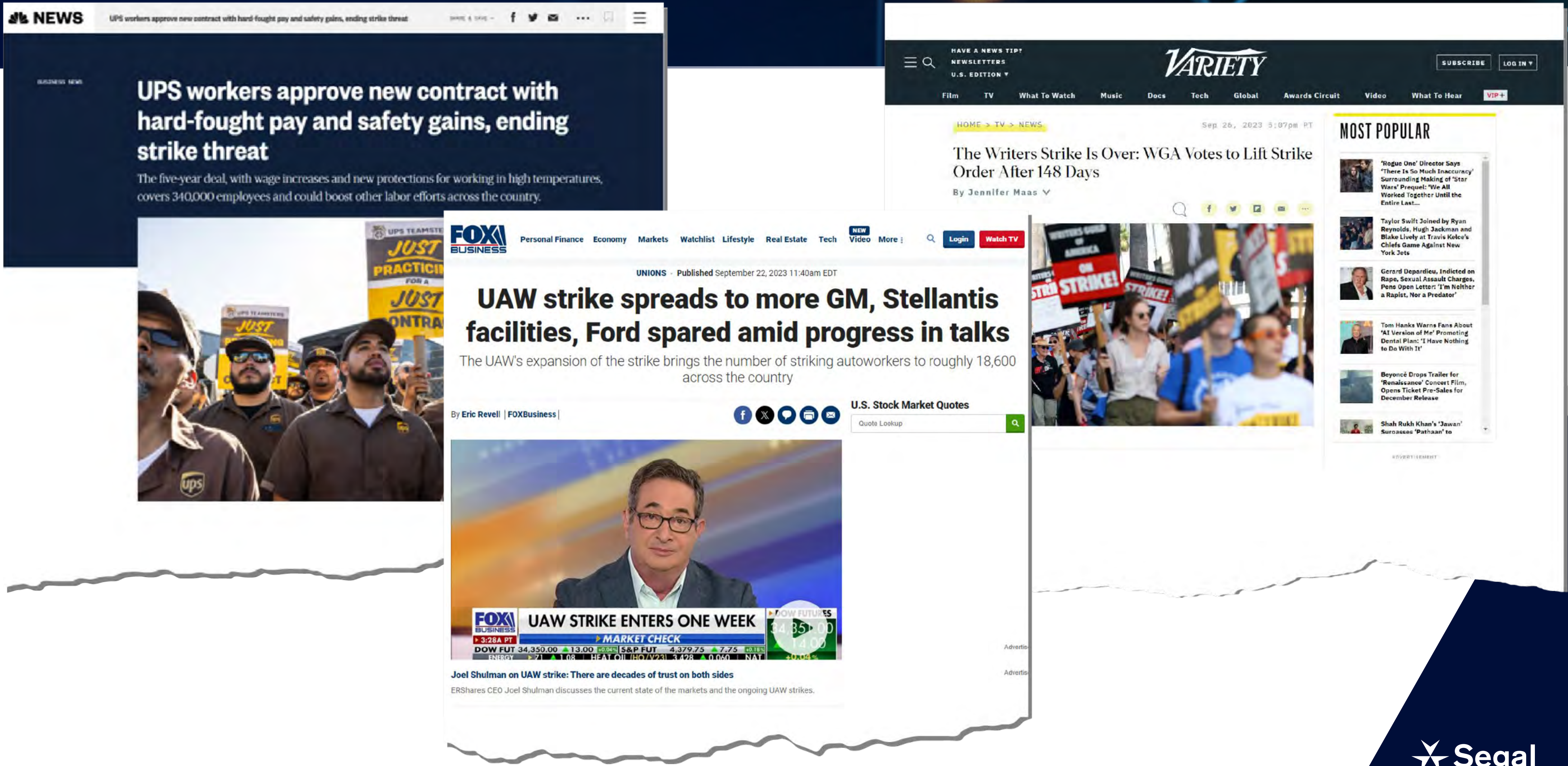
The three largest sectors of multiemployer plan sponsors (food, construction and trucking) will go through profound changes over the next twenty years

Technology

Artificial Intelligence

Disruptive Innovation

Strikes and Negotiations



NEWS

UPS workers approve new contract with hard-fought pay and safety gains, ending strike threat

BUSINESS NEWS

UPS workers approve new contract with hard-fought pay and safety gains, ending strike threat

The five-year deal, with wage increases and new protections for working in high temperatures, covers 340,000 employees and could boost other labor efforts across the country.

FOX BUSINESS

Personal Finance Economy Markets Watchlist Lifestyle Real Estate Tech NEW Video More Login Watch TV

UNIONS · Published September 22, 2023 11:40am EDT

UAW strike spreads to more GM, Stellantis facilities, Ford spared amid progress in talks

The UAW's expansion of the strike brings the number of striking autoworkers to roughly 18,600 across the country

By Eric Revell | FOXBusiness |

U.S. Stock Market Quotes

Quote Lookup

FOX BUSINESS
3:28A PT
UAW STRIKE ENTERS ONE WEEK
MARKET CHECK
DOW FUT 34,350.00 ▲13.00 S&P FUT 4,379.75 ▲7.75
DOW FUTURES

Joel Shulman on UAW strike: There are decades of trust on both sides

ERShares CEO Joel Shulman discusses the current state of the markets and the ongoing UAW strikes.

HAVE A NEWS TIP?
NEWSLETTERS
U.S. EDITION

VARIETY

SUBSCRIBE LOG IN

Film TV What To Watch Music Docs Tech Global Awards Circuit Video What To Hear VIP+

HOME > TV > NEWS

Sep 26, 2023 5:07pm PT

The Writers Strike Is Over: WGA Votes to Lift Strike Order After 148 Days

By Jennifer Maas

MOST POPULAR

'Rogue One' Director Says 'There Is So Much Inaccuracy' Surrounding Making of 'Star Wars' Prequel: 'We All Worked Together Until the Entire Last...

Taylor Swift Joined by Ryan Reynolds, Hugh Jackman and Blake Lively at Travis Kelce's Chiefs Game Against New York Jets

Gerard Depardieu, Indicted on Rape, Sexual Assault Charges, Pens Open Letter: 'I'm Neither a Rapist, Nor a Predator'

Tom Hanks Warns Fans About 'AI Version of Me' Promoting Dental Plan: 'I Have Nothing to Do With It'

Beyoncé Drops Trailer for 'Renaissance' Concert Film, Opens Ticket Pre-Sales for December Release

Shah Rukh Khan's 'Jawan' Surpasses 'Pathaan' to

ADVERTISEMENT

Thank You

David Brenner

SVP and National Director of Multiemployer Consulting

dbrenner@segalco.com

617-424-7330

Multiemployer IT Summit

What's NExT?

Artificial Intelligence, Your Organization and You

Randi Farber, Gokul Sheshadri & Michael Stoyanovich

October 10-11, 2023 / San Diego

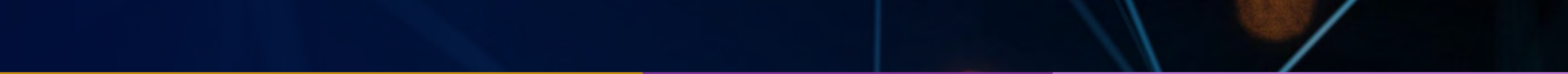
Proudly sponsored by

Segal

Agenda

- What is AI (really)?
- What are the risk and threats?
- If you want to use AI, establish a method to govern it
- Two Use Cases

What is Artificial Intelligence (AI)?



“It’s like collaborating with an alien.”

“It feels like I’ve hired an intern.”

“What used to take me around a half-hour to write now takes one minute.”

“It’s enormous fun.”

“Everything is becoming much easier”

From the New York Times “35 Ways Real People Are Using A.I. Right Now” by Francesca Paris and Larry Buchanan April 14, 2023

Artificial Intelligence

What is AI?

Any computing system designed to perform tasks that normally require human intelligence

In general, how does AI work?

These systems: Ingest large amounts of (training) data, analyze it for patterns (via a neural network), then use these patterns to make predictions (via statistical models)

These Technologies are All Artificial Intelligence

Machine Learning

Algorithms trained to detect patterns and make predictions (e.g. Netflix recommendations)

“Deep Learning”

A type of ML that uses neural networks to learn from vast amounts of data for more complex applications (e.g. self-driving cars)

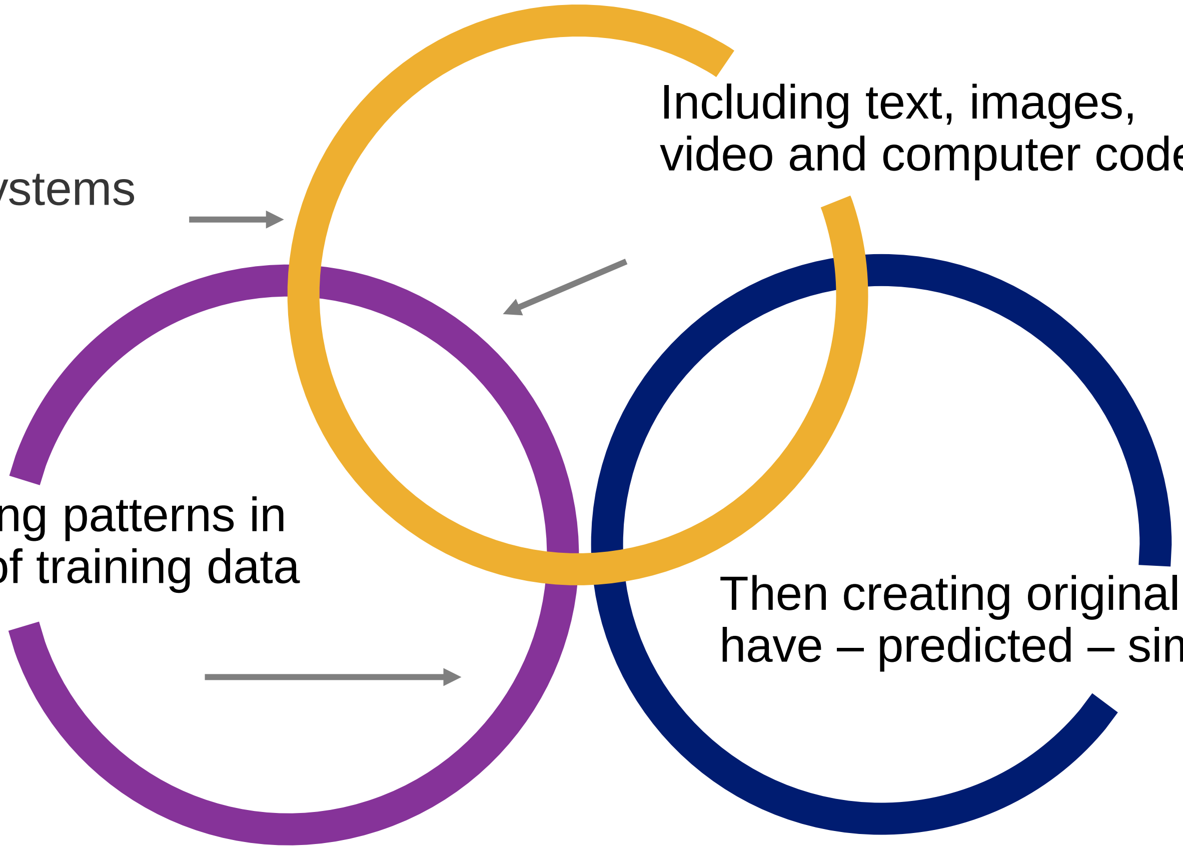
Natural Language Processing

Helps computers understand human language (e.g. Email filters)

Generative AI

Large language model (LLM) based applications that create new text, images, video, and audio. This is the “AI” that is garnering all the attention

Generative AI Has Captured The Most Public Attention



Generative AI systems *create* content

Including text, images, video and computer code

How? By identifying patterns in large quantities of training data

Then creating original material that have – predicted – similar characteristics.

That is a key fact for you to understand, these systems are generating output based on statistical model based predictions. There is no actual 'computer intelligence' involved.

The First Widely Used Generative AI? Chat Application(s)

Traditional Chatbots

- Low complexity
- Basic answer and response machines
- Based on limited scope of training data and information
- Need training for every scenario (not “intelligent”)

AI-Powered Chatbots

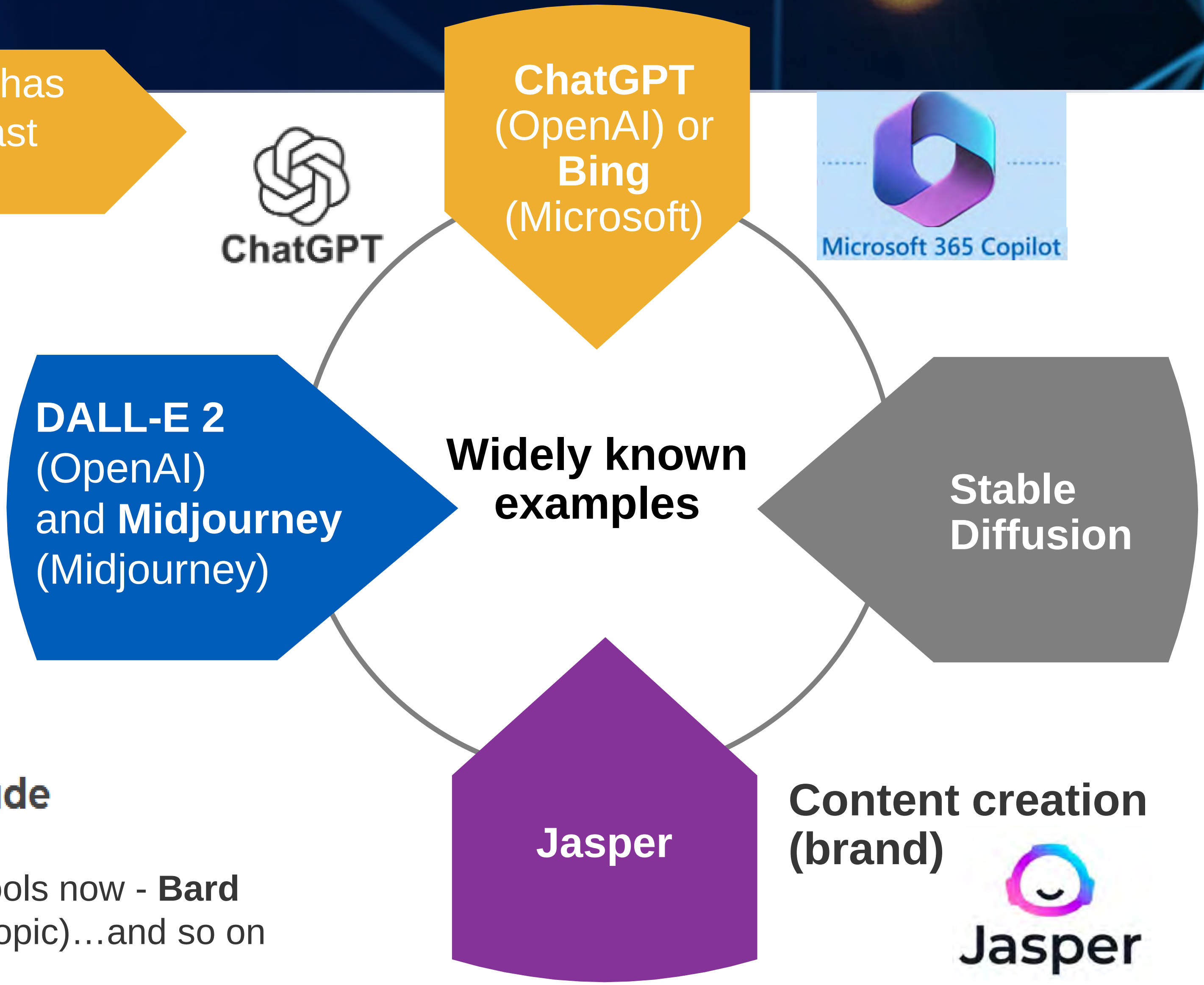
- Manage complex dialogues
- Based on *much* larger scope of training data and information (the whole public web)
- Contextually aware and *seemingly* “intelligent”
- Can self-learn and improve predictions over time

These Are Illustrative Generative AI Tools

Use of GenAI tools has exploded in the past 10 months!

ChatGPT

Microsoft 365 Copilot



ChatGPT (OpenAI) or **Bing** (Microsoft)

DALL-E 2 (OpenAI) and **Midjourney** (Midjourney)

Widely known examples

Stable Diffusion

Jasper

Images

Midjourney

Realistic images and videos

Stable Diffusion

Content creation (brand)

Jasper

Bard

Claude

There are *many* public tools now - **Bard** (Google), **Claude** (Anthropic)…and so on and so forth

Artificial Intelligence Myth Busting

NOT

Sentient*

Generative AI is not self-aware.

It is not Artificial *General* Intelligence (AGI)

NOT

Robotics

NOT

The problem-solving tool

You (the human) still have to know how to formulate a problem to get good results

NOT

Interpretive

GenAI cannot use common sense or understand nuances like humans can

NOT

The decision-making tool

You (the human) still have to apply critical thinking to the output.

Does this make sense?

*"Roughly speaking, they take huge amounts of data, search for patterns in it and become increasingly proficient at generating statistically probable outputs — such as seemingly *humanlike* language and thought."

Noam Chomsky - New York Times, March 8, 2023

What are the risks and threats?

If you want to use AI, establish a method to govern it

Risks and Threats of AI: There Are Many

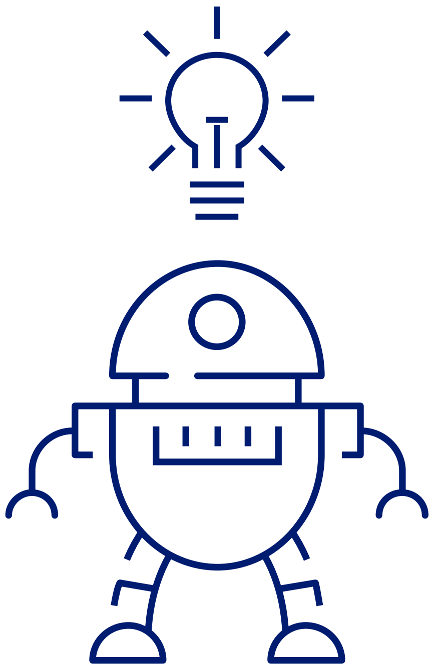
All of these risks and threats (to name some), need be managed, by your organization when using AI

- Misinformation
- Embedded Bias
- Privacy Protection
- Security Controls
- Intellectual Property (IP) Issues
- Ethical Considerations
- Legal Issues
- Regulations
- Bad Optics (PR)

Hallucinations

Risks and Threats: Taking AI on Faith

- GenAI tools, in particular, are not doing what you may think they are doing
- Reminder AI is not *thinking**
- As noted previously, AI tools are designed to learn from very large datasets and generative AI tools are meant to create new content based on that data (in combination with the model (neural network)). They are not capable of understanding the nuances of human language and culture in the same way that humans are
- Therefore, unsurprisingly, they sometimes produce nonsensical (but believable) responses, which includes just “making things up” (aka hallucinations)



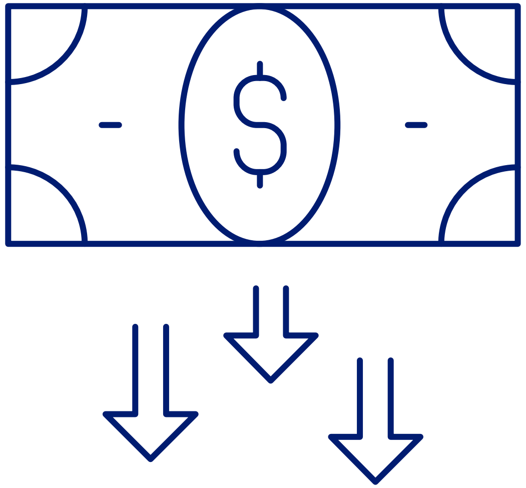
* At least not in any common use understanding of what “thinking” means.

Remember This Newsworthy Hallucination?

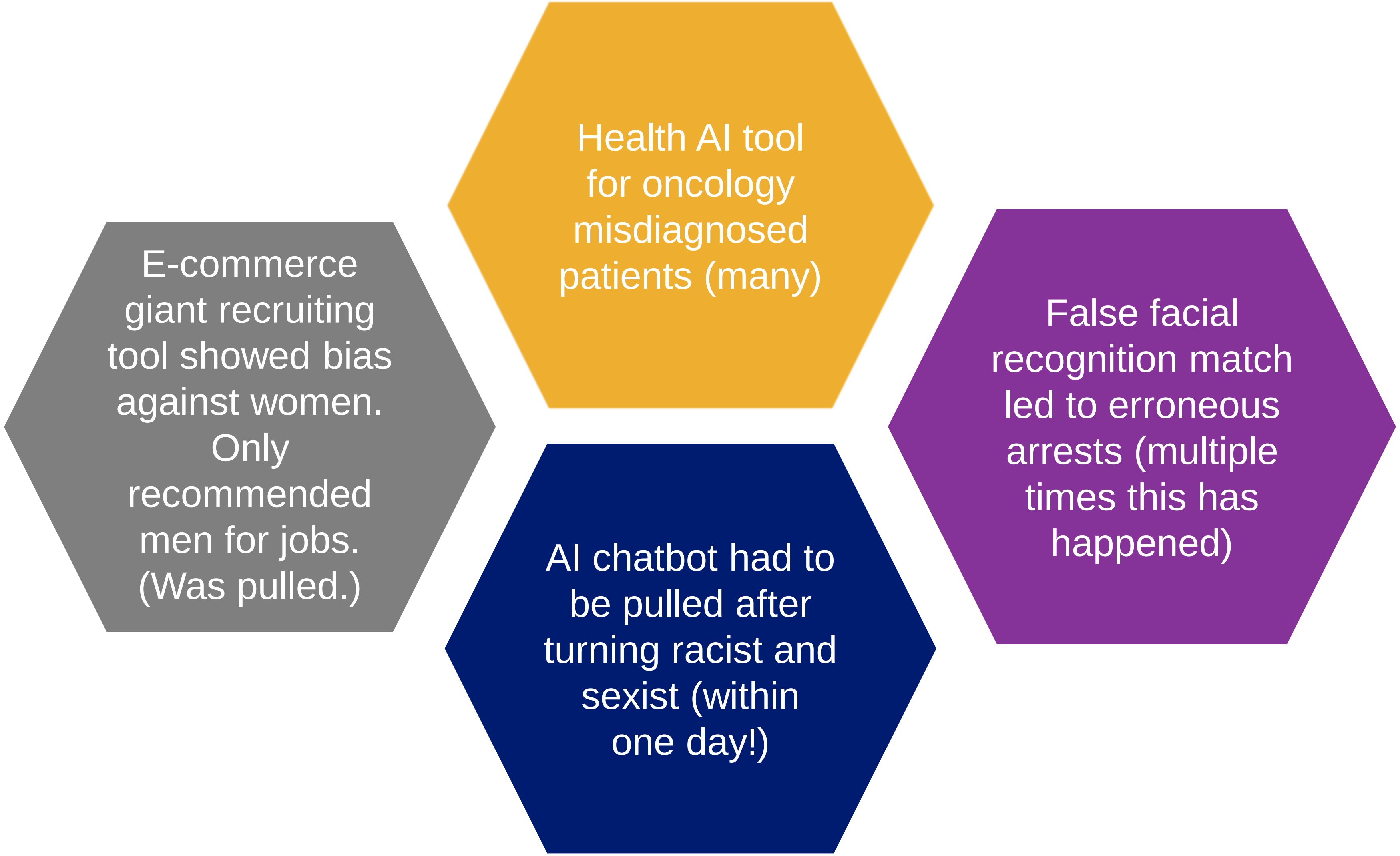
- Lawyers who cited fake cases hallucinated by ChatGPT must pay
- Judge sanctions attorneys for failed reality check

“Attorneys who filed court documents citing cases completely invented by OpenAI's ChatGPT have been formally slapped down by a New York judge.”

– The Register June 22, 2023



Other Real-Life Illustrations of AI Failures



E-commerce giant recruiting tool showed bias against women. Only recommended men for jobs. (Was pulled.)

Health AI tool for oncology misdiagnosed patients (many)

AI chatbot had to be pulled after turning racist and sexist (within one day!)

False facial recognition match led to erroneous arrests (multiple times this has happened)

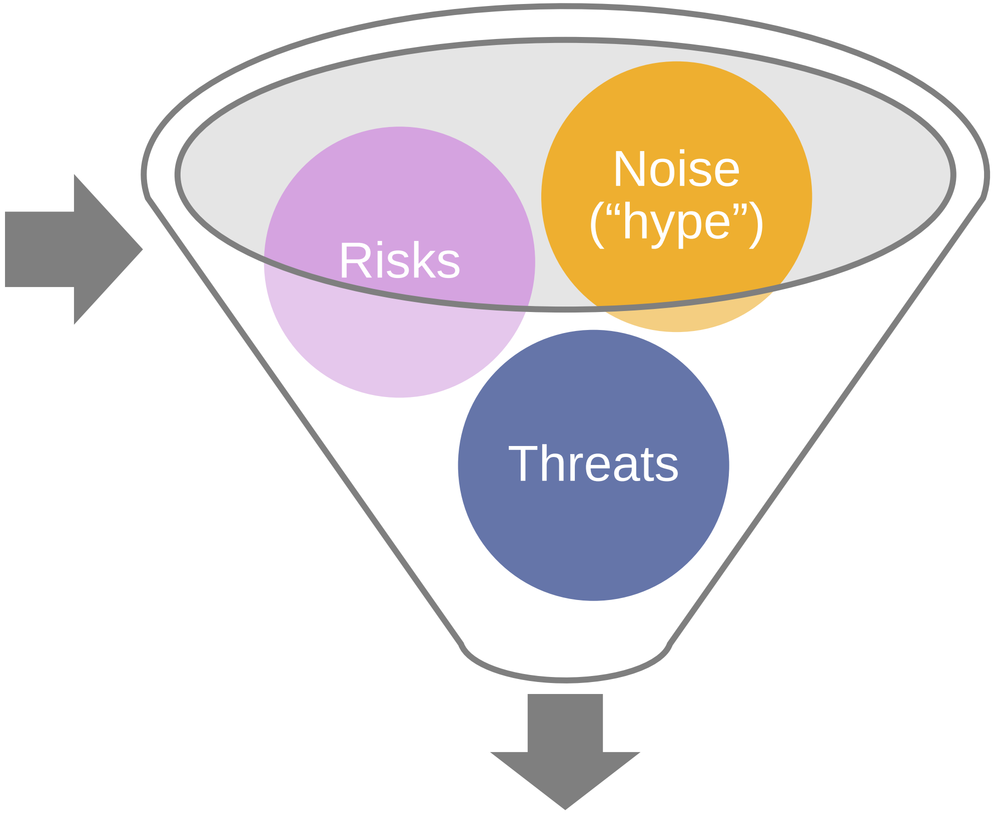
Potentially The Most Significant Risk or Threat?

AI may lull people and organizations into the false sense of security that they don’t have to use their critical thinking skills

Leading them to…**Do dumb things…Faster (with AI)**

Yet…AI Cannot, and *Should Not*, be Ignored by Organizations

All this may be true, yet you still should embrace AI prospectively



Ignore at Your Own Peril
AI won't replace humans, but humans *with* AI will replace humans without AI

**You should still be exploring
how to use AI in your organization (and for yourself)**

If you want to use AI, establish a method to govern it.

First Step

Before you start using any AI tools within your organization, think about and then establish how you will govern AI

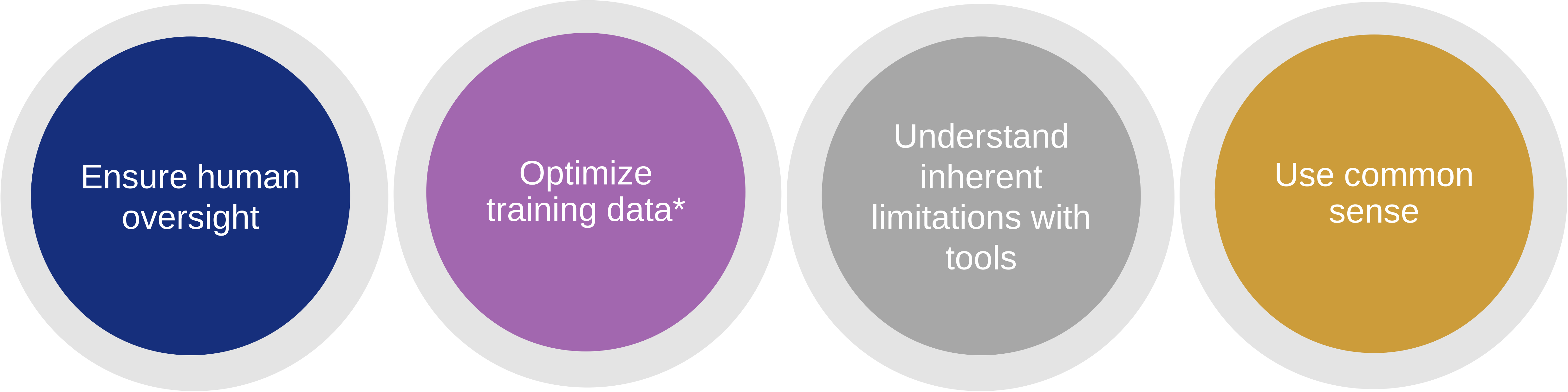
Governance for Generative AI

- Create a clear policy on acceptable use of authorized tools
- Communicate the benefits and risks (there are both)
- Train staff on tools that are authorized (and note categories and tools that are not authorized)
- Ensure transparency and accountability by individuals and the organization, as a whole
- Implement controls to protect data from unauthorized access or misuse

Governance for Generative AI

- Address broader privacy, cybersecurity, bias and ethical considerations
- Monitor for compliance with applicable laws and regulations (continuously, as they will change)
- Review and update the governance policy regularly as technology, laws, and ethical standards of use all evolve

Managing Generative AI Outputs



Ensure human oversight

Optimize training data*

Understand inherent limitations with tools

Use common sense

* If you are going to produce your own generative AI tool (LLM based) you must consider training data (and the model (neural network)) to ensure no intellectual property infringement, ethical or other concerns are "baked into" your tool.

Two Use Cases

32 BJ

- The Building Service 32BJ Benefit Funds provide comprehensive and affordable benefits to its members. As part of its efforts to improve our members' experience and engagement, the Funds are considering using the ChatGPT Application Programming Interface (API) to enable a member portal chatbot that can respond to specific questions about the benefits provided by the Funds.
- The ChatGPT API is a powerful tool that enables 32BJ to build intelligent chatbots that can connect with participants and provide useful information. 32BJ is performing a proof of concept to see if it will leverage this technology to improve the accessibility and responsiveness of its member portal, enabling members to easily find the information they need to obtain, use, or manage their benefits without compromising security or accuracy.

SAG-AFTRA

- The SAG-AFTRA Health Plan is a multi-employer health plan for members of the SAG-AFTRA, the Union. It provides medical, dental, and vision benefits, as well as mental health benefits, to support the well-being of performers, media professionals, and their families within the entertainment industry.
- The SAG Producers Pension Plan is a retirement program for SAG-AFTRA members. This plan assists in ensuring the financial well-being of performers once their careers in the entertainment industry have concluded.
- The Plans are exploring using AI power tools to interrogate interactions between end users of its contact center, web properties, etc., for sentiment analysis in "real time" (alerting supervisors of potentially negative interactions), and to offer suggested – new- topics for end user self-help materials on public properties, based on what they are contacting the organization to inquire about.

Thank You

For more info, please contact us

Randi Farber
Director, Technology & Operations,
Building Service 32BJ Benefit Funds

Gokul Sheshadri
COO, SAG AFTRA Plans

Michael Stoyanovich
VP and Senior Consultant, Segal
Consulting’s Administration &
Technology Consulting Practice

Multiemployer IT Summit

What's NExT?

How Much More to Get to Zero

Cameron Matthews, vCISO
Nth Generation

October 10-11, 2023 / San Diego

Proudly sponsored by
Segal

Agenda

1. Zero Trust (ZT): What and Why?
2. ZT Conceptual Overview
3. Security Journey
4. ZT Journey
5. Challenges
6. First Steps
7. Key Takeaways
8. Q&A

Zero Trust (ZT): What and Why?

What is Zero Trust?

Why do we need it?

Security History

- We made bad assumptions that led to bad outcomes
- We assumed that resources (users, devices, network components) that we had inside our network could be implicitly trusted.
- We were wrong

Threats exist inside the network as well as outside

- Hackers
- Insider Threat
  - Disgruntled employees
  - Foreign nation-states
  - Competitors

Security Present

- We can no longer depend on conventional perimeter-based defenses
- The security perimeter has exploded, is no longer hardware or property delineated, and has gone virtual and mobile
- Assets have evolved beyond the network
  - Off-network assets — BYOD, WFH, Mobile, and SaaS
  - Service and protocol changes have outpaced tools & expertise
- Attackers have shifted to identity attacks
  - Phishing/vishing/smishing
  - Credential theft/reuse
  - BEC

Security Future (with ZT)

- Single source of ground truth for **identity** that is validated by strong, social engineering-resistant authentication
- Complete visibility of **devices** accessing the extended network with strict access policies around compliance and health status
- **Application** authorization (privileges) dynamically minimized based on contextual and behavioral real-time analytics. App development using SSDLC exclusively.
- Continuous **data**-driven protection through automated and dynamic classification, labeling, analytics, access minimization, and encryption decisions.

Security Future (with ZT)

- Advanced **infrastructure** telemetry usage to detect anomalous behaviors and known attacks for autonomous blocking. Automated flagging of risky behavior by users and devices. Universal enforcement of least privilege

- No implicit trust of devices or users on the **network**: strong authentication required for all access. Encryption of all communications. Access of networked resources based dynamically-evaluated policies. Dynamic resilience in the face of network resource challenges.

- **Cross-cutting capabilities** including visibility and analytics, automation and orchestration, and governance

ZT Reality Check

- ZT is an approach, an idea, and a set of goals
- As such, the ultimate “Zero Trust” (as in, nothing is assumed trusted) may not be achievable. And you may not *want* to achieve it
- Security and usability, convenience, and performance are usually inversely related. Going in either direction has negative consequences
- You must define what your “inner circle” is, how far you want to take ZT, and how much you can do based on resources and enterprise impact

ZT Conceptual Overview

Definitions

Guiding Principles

Pillars

Definitions

ZT: collection of concepts and ideas to enforce least-privilege, per-request access decisions in the face of a compromised network (NIST)

ZT: is a security model, a set of system design principles, a cybersecurity and system management strategy, and a mindset (NSA)

ZTA: enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies (NIST)

ZTNA: a [capability] that creates an identity- and context-based, logical access boundary around applications. Access is only granted to strongly-authenticated entities via a trust broker that dynamically validates identity, context, and policy (Gartner)

Guiding Principles

Never Trust, Always Verify

- Every user, device, application/workload, and data flow as untrusted
- Authenticate and authorize each of these according to least privilege

Assume Breach

- Always act as if a breach occurred and hackers are in networks and on hosts
- Deny by default
- Monitor all behavior for anomalies

Verify Explicitly

- Make no assumptions about identity, authentication, authorization
- Validate access by context using multiple attributes both static and dynamic

Pillars

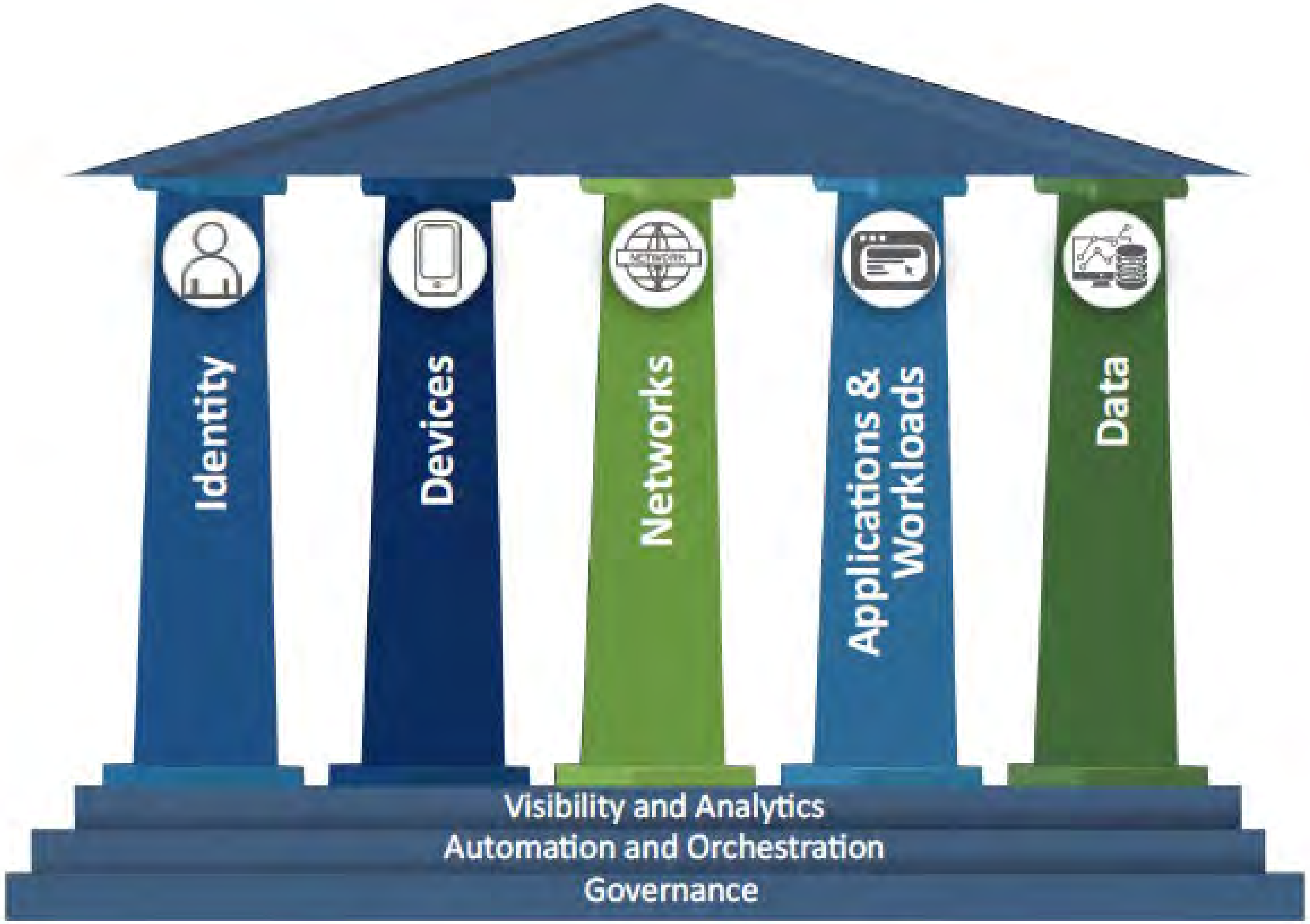


Figure 1: Zero Trust Maturity Model Pillars[8]

Pillars Detail

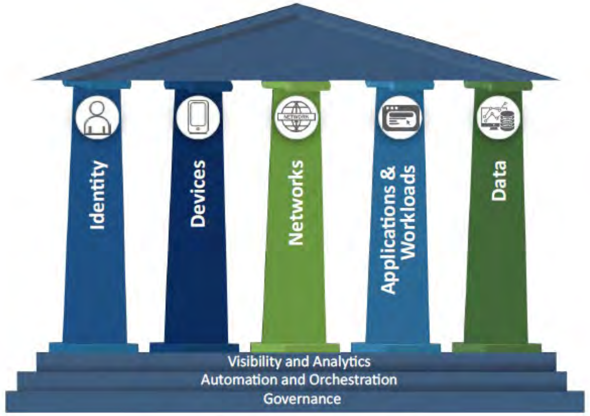


Figure 1: Zero Trust Maturity Model Pillars[8]

Identity

An attribute or set of attributes that uniquely describes a user or entity, including non-person entities (e.g. device)

Devices

Any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more

Networks

Typical communications channels such as internal wired networks, wireless networks, and the Internet as well as cellular and application-level channels used to transport messages.

Pillars Detail

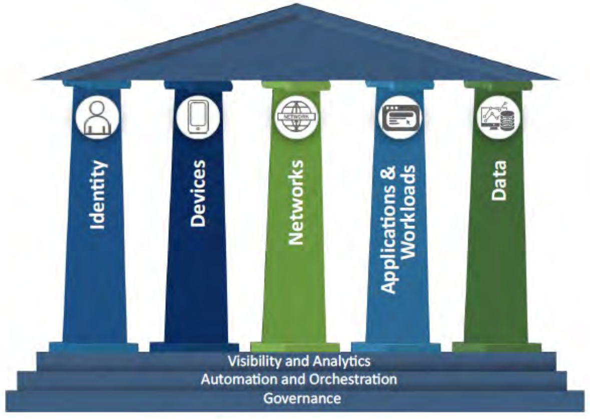


Figure 1: Zero Trust Maturity Model Pillars[8]

Applications and Workloads

Systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments

Data

All structured/unstructured files/data that reside or have resided in systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata

Cross-cutting Capabilities

- Visibility and Analytics
- Automation and Orchestration
- Governance

Security Journey

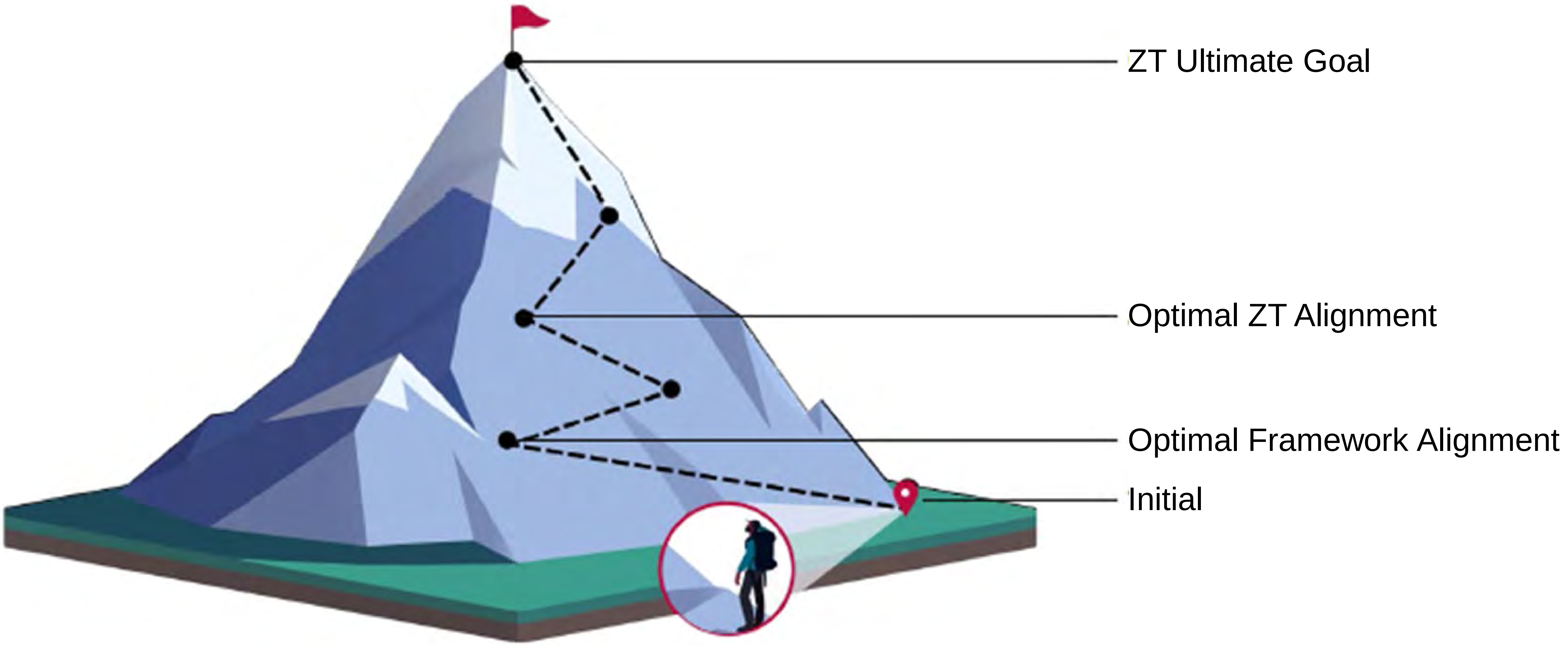
Security Journey

Security Journey concept and Maturity Models

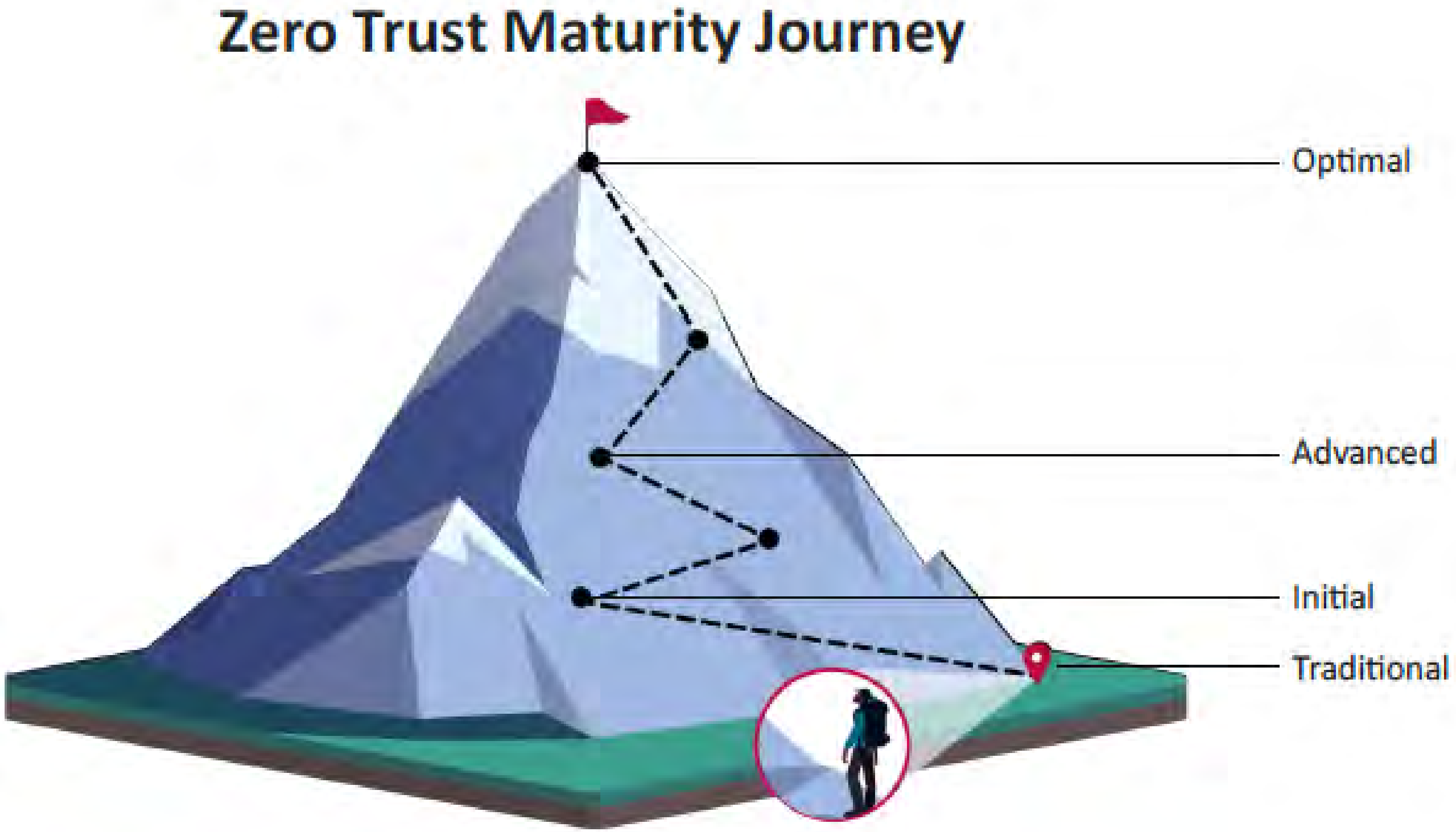
ZT Journey and the “Traditional” Security Journey

Inverting/reversing Perspective

Security Journey (Cameron)



ZT Journey (CISA)



Zero Trust Maturity Journey

Figure 2: Zero Trust Maturity Journey

“Traditional” Cybersecurity Frameworks

CIS CSC

Applicable to a wide variety of organizations both commercial and public sector

NIST CSF

U.S. Critical Infrastructure, high Operational Technology (OT)

NIST 800-53/RMF

Department of Defense

NIST 800-171/CMMC

Federal/DoD contractors that process certain types of government data

ISO 27000 series

ZT Maturity Journey (CISA, per Pillar)

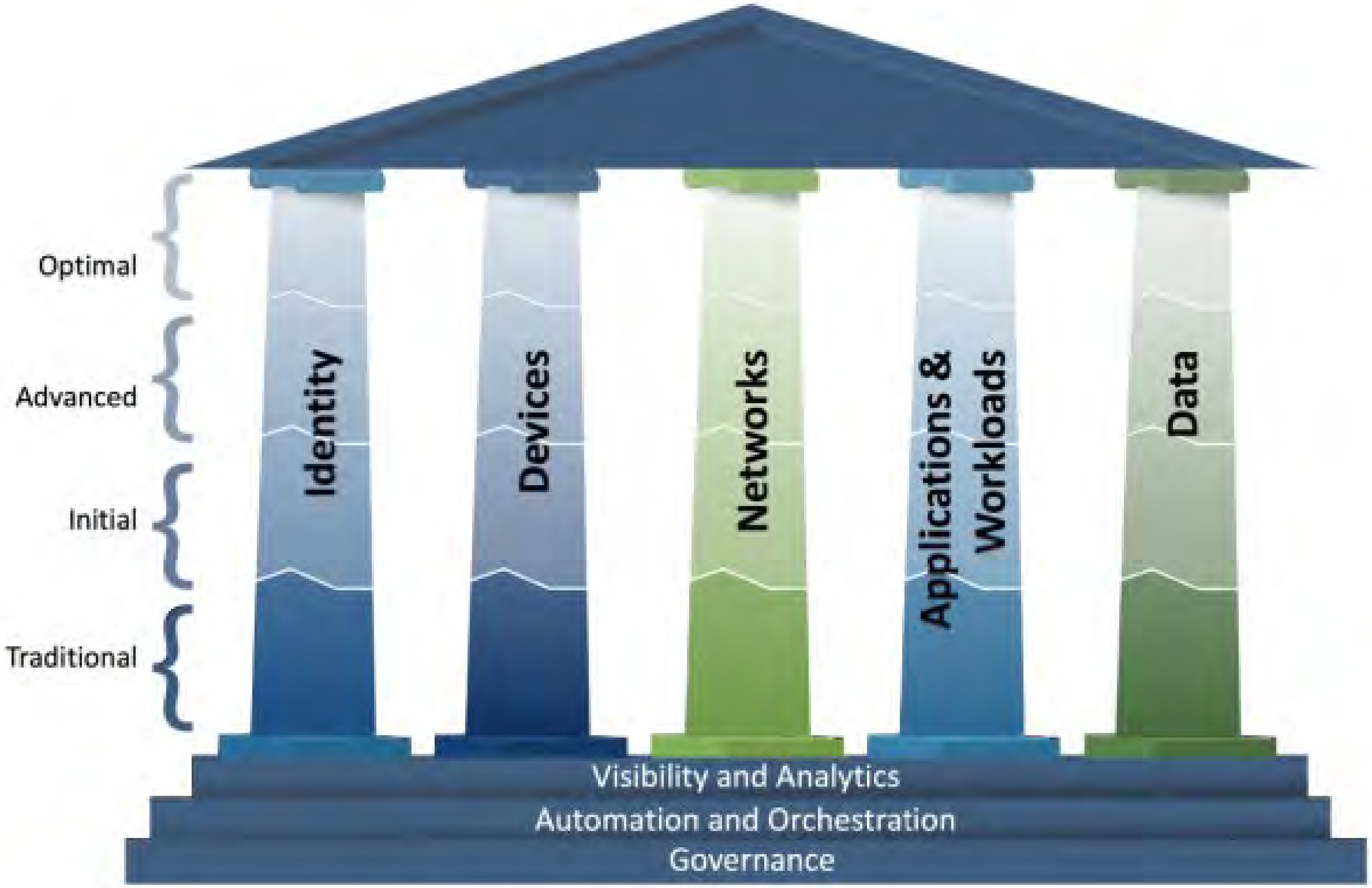
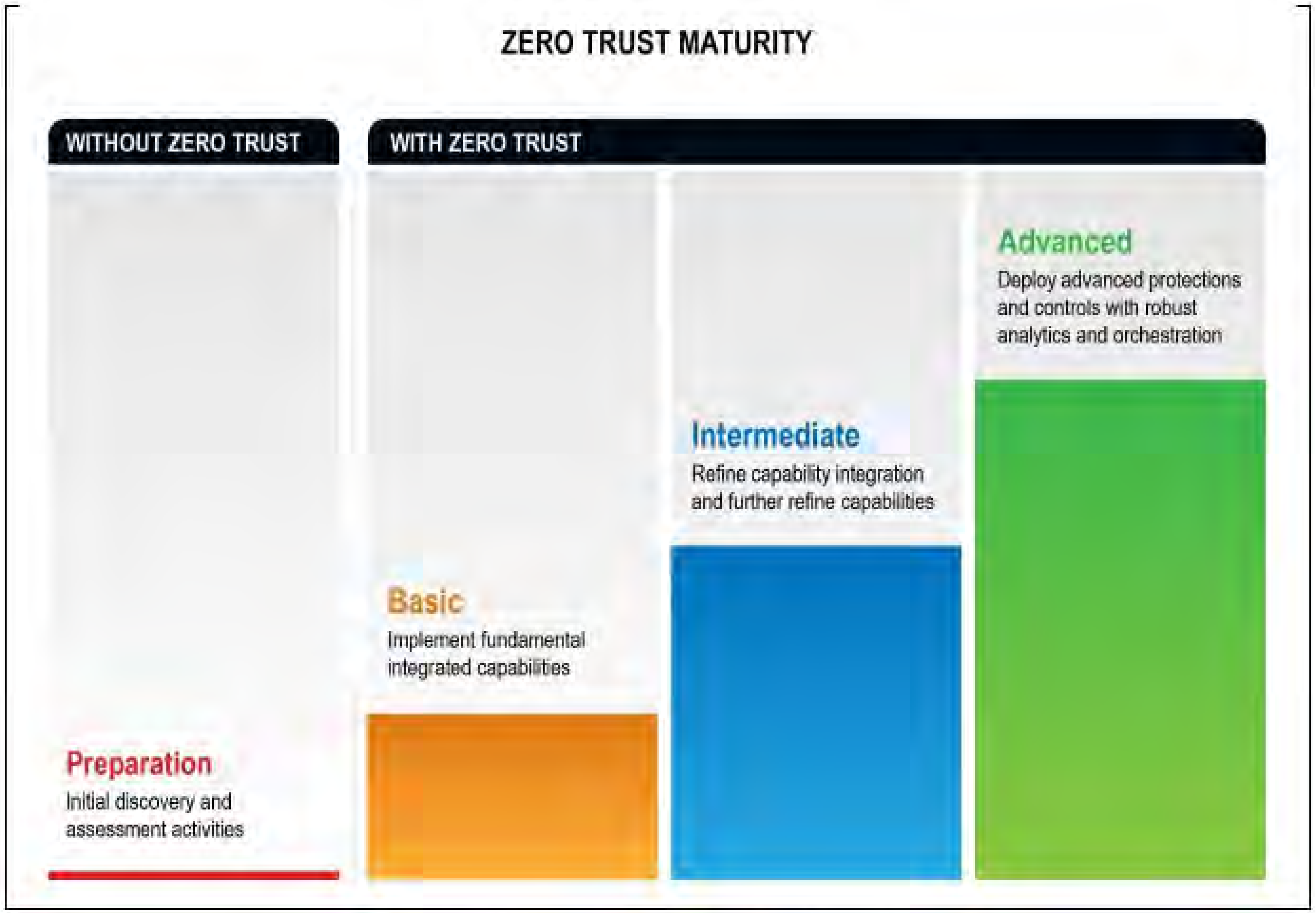


Figure 3: Zero Trust Maturity Evolution

ZT Maturity Journey (NSA)



ZERO TRUST MATURITY

WITHOUT ZERO TRUST

WITH ZERO TRUST

Preparation
Initial discovery and assessment activities

Basic
Implement fundamental integrated capabilities

Intermediate
Refine capability integration and further refine capabilities

Advanced
Deploy advanced protections and controls with robust analytics and orchestration

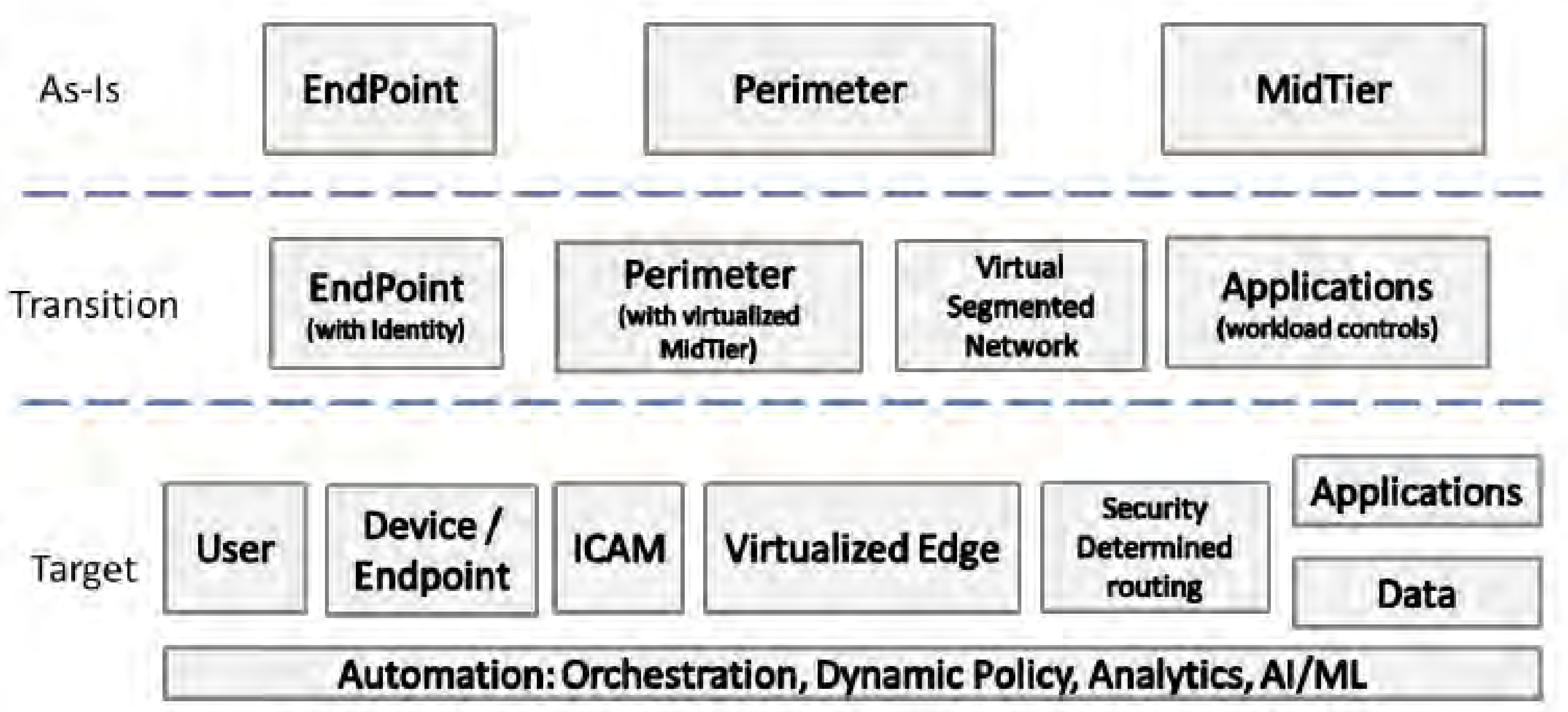
Figure 2: Maturing a Zero Trust implementation

ZT Journey (US Federal)

M-22-09 Federal Zero Trust Strategy, strategic goals for each Pillar

- 1. **Identity:** Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
- 2. **Devices:** The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
- 3. **Networks:** Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
- 4. **Applications and Workloads**: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
- 5. **Data**: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

ZT Journey (Dept of Defense)



As-Is

EndPoint

Perimeter

MidTier

Transition

EndPoint (with Identity)

Perimeter (with virtualized MidTier)

Virtual Segmented Network

Applications (workload controls)

Target

User

Device / Endpoint

ICAM

Virtualized Edge

Security Determined routing

Applications

Data

Automation: Orchestration, Dynamic Policy, Analytics, AI/ML

Figure 44 Transition Architecture Transition (OV-1)

ZT Journey (NSA)

Adopt a Zero Trust mindset

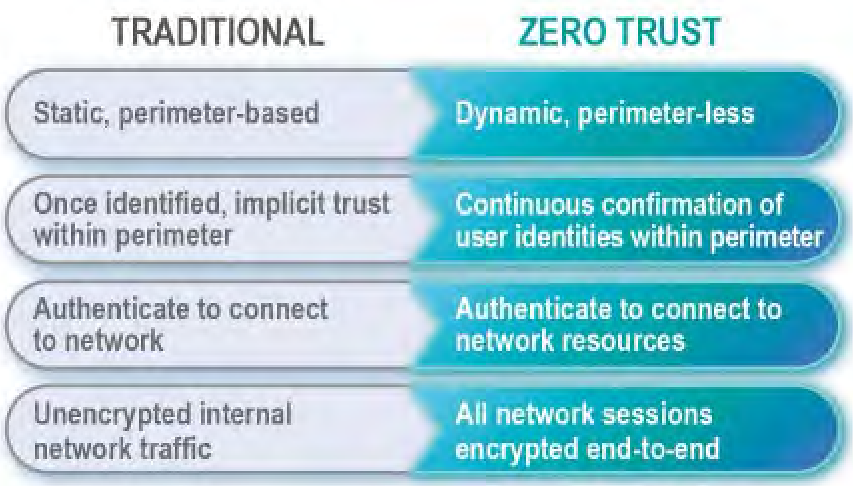
- Coordinated and aggressive system monitoring, system management, and defensive operations capabilities
- Assuming all requests for critical resources and all network traffic may be malicious
- Assuming all devices and infrastructure may be compromised
- Accepting that all access approvals to critical resources incur risk, and being prepared to perform rapid damage assessment, control, and recovery operations

ZT Journey (NSA)

Leverage Zero Trust design concepts

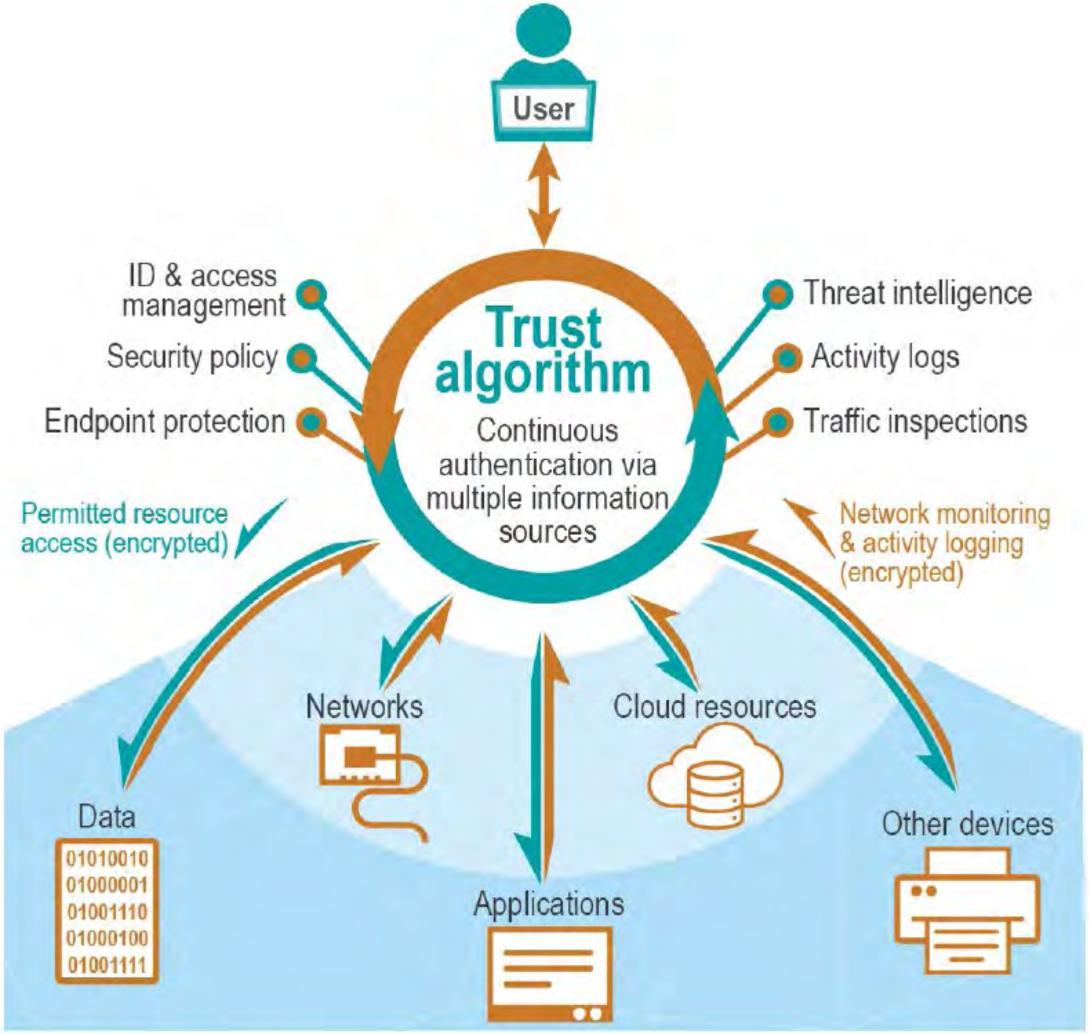
- Define mission outcomes – Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).
- Architect from the inside out – First, focus on protecting critical DAAS. Second, secure all paths to access them.
- Determine who/what needs access to the DAAS to create access control policies – Create security policies and apply them consistently across all environments (LAN, WAN, endpoint, perimeter, mobile, etc.).
- Inspect and log all traffic before acting – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.

ZT Journey (GAO)



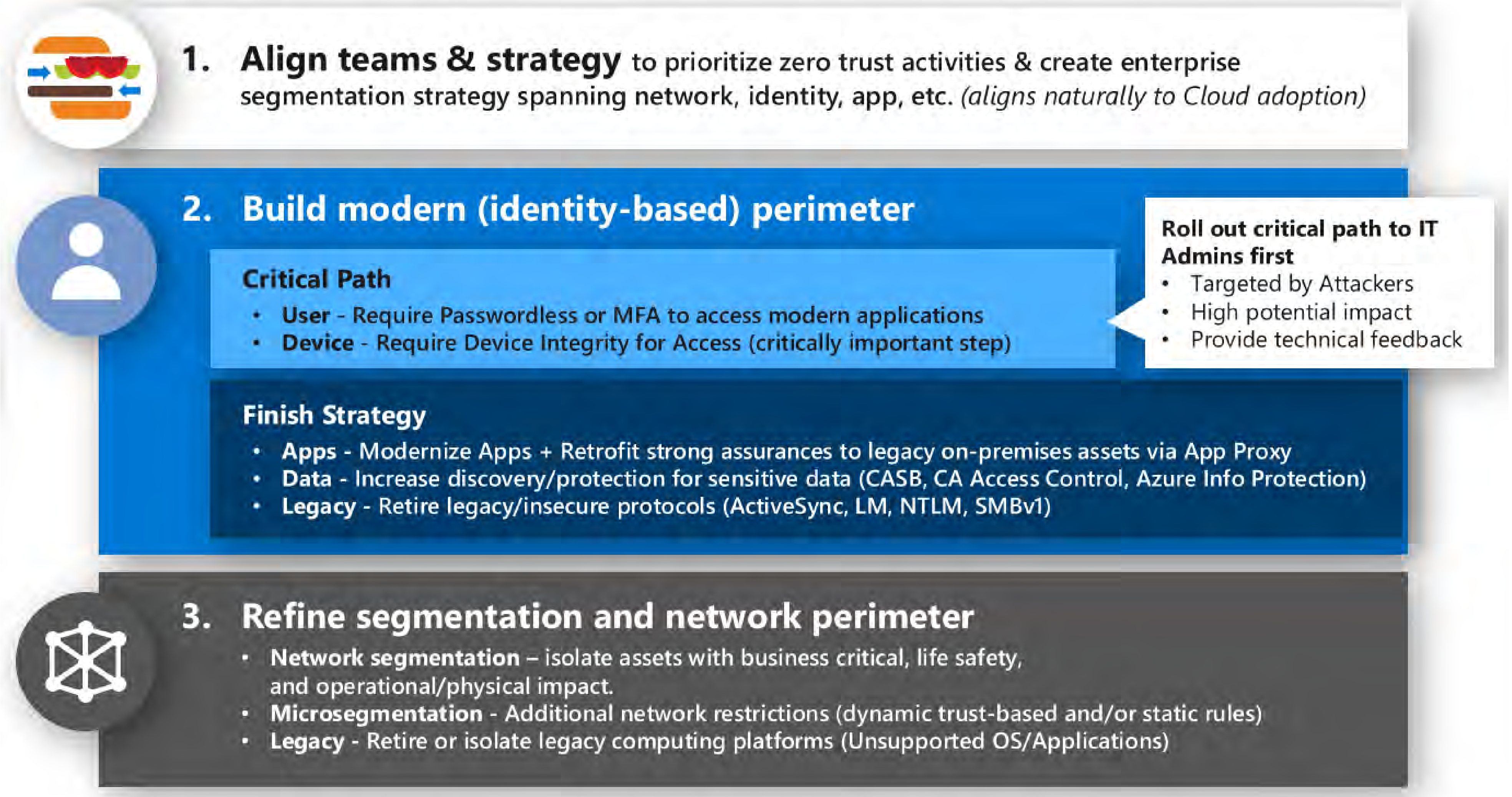
TRADITIONAL	ZERO TRUST
Static, perimeter-based	Dynamic, perimeter-less
Once identified, implicit trust within perimeter	Continuous confirmation of user identities within perimeter
Authenticate to connect to network	Authenticate to connect to network resources
Unencrypted internal network traffic	All network sessions encrypted end-to-end

Source: GAO analysis of industry sources. | GAO-23-106065



Source: GAO analysis of NIST documentation. | GAO-23-106065

ZT Journey (Microsoft's RAMP)



1. **Align teams & strategy** to prioritize zero trust activities & create enterprise segmentation strategy spanning network, identity, app, etc. *(aligns naturally to Cloud adoption)*

2. **Build modern (identity-based) perimeter**

Critical Path

- **User** - Require Passwordless or MFA to access modern applications
- **Device** - Require Device Integrity for Access (critically important step)

Roll out critical path to IT Admins first

- Targeted by Attackers
- High potential impact
- Provide technical feedback

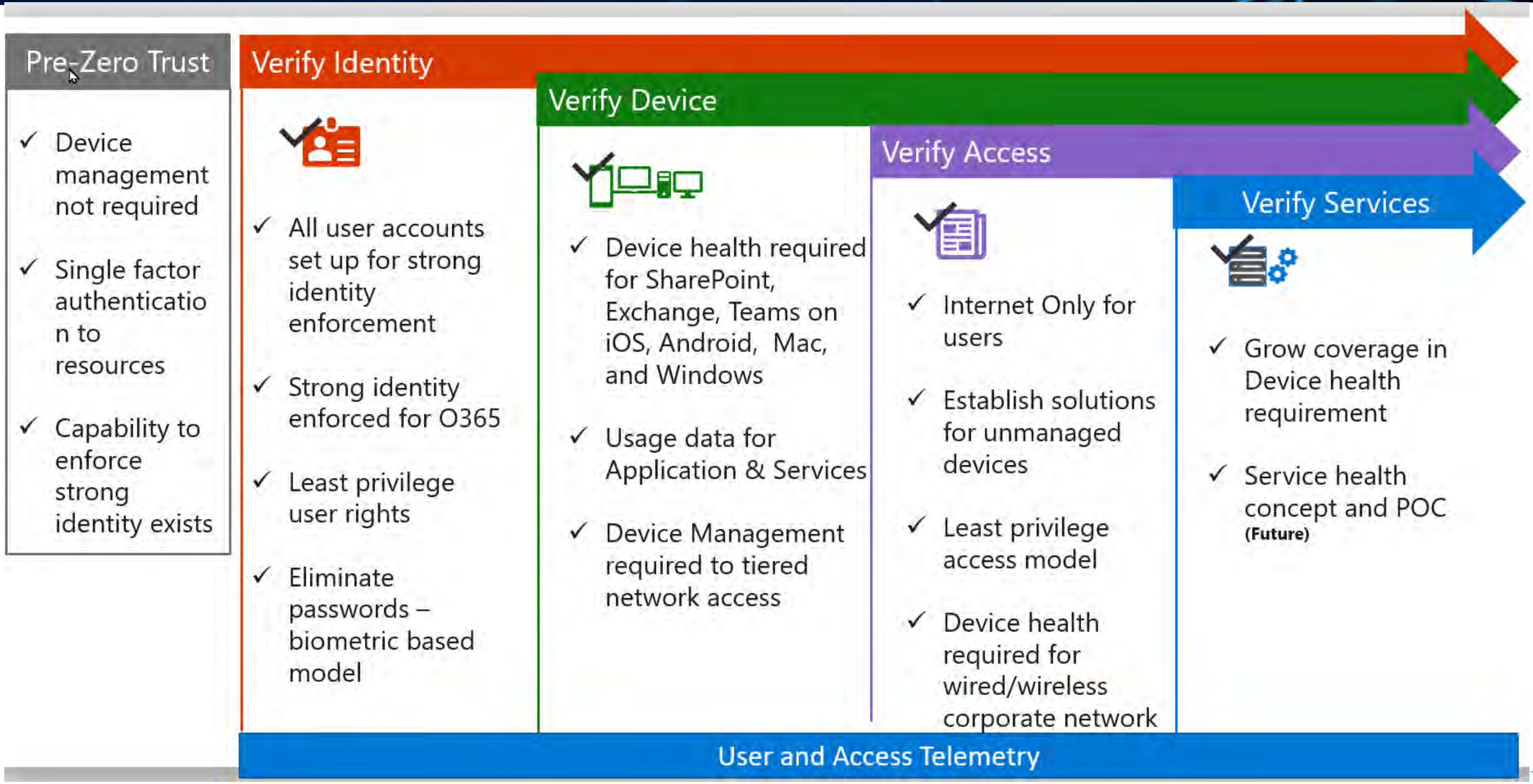
Finish Strategy

- **Apps** - Modernize Apps + Retrofit strong assurances to legacy on-premises assets via App Proxy
- **Data** - Increase discovery/protection for sensitive data (CASB, CA Access Control, Azure Info Protection)
- **Legacy** - Retire legacy/insecure protocols (ActiveSync, LM, NTLM, SMBv1)

3. **Refine segmentation and network perimeter**

- **Network segmentation** – isolate assets with business critical, life safety, and operational/physical impact.
- **Microsegmentation** - Additional network restrictions (dynamic trust-based and/or static rules)
- **Legacy** - Retire or isolate legacy computing platforms (Unsupported OS/Applications)

ZT Journey (Microsoft's Major Phases)



Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists

Verify Identity

- ✓ All user accounts set up for strong identity enforcement
- ✓ Strong identity enforced for O365
- ✓ Least privilege user rights
- ✓ Eliminate passwords – biometric based model

Verify Device

- ✓ Device health required for SharePoint, Exchange, Teams on iOS, Android, Mac, and Windows
- ✓ Usage data for Application & Services
- ✓ Device Management required to tiered network access

Verify Access

- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for wired/wireless corporate network

Verify Services

- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Future)**

User and Access Telemetry

Challenges

Challenges

- No complete, turnkey, single vendor solution
- Organizational resistance (IT, security, workers)
  - IT: tired of redesign, constant integration, breach assumption, etc.
- Lack of Executive Buy-in
  - Budget, leadership through example
- Redesign of IT systems and networks can take considerable time and effort
- Legacy systems: replace, integrate, or evolve?

Challenges

- ZT as a pursuit and discipline is rapidly evolving.
  - There is no single true standard
  - The “standards” and approaches will continue to change over time
  - Monitor and maintain awareness
  - Be flexible and adaptable
- ZT was ill-defined in the beginning so it’s definition and discipline vary from organization (CISA) to organization (NSA) to organization (GAO).
- For vendors, ZT solutions/products/services may not integrate or interoperate well.

First Steps

First Steps

✓ Assess your current “Traditional” cybersecurity posture

- Choose an applicable “Traditional” cybersecurity framework
- Perform an assessment
- Determine current posture
- Identify gaps based upon chosen target

✓ Determine your acceptable smallest, inner circle of implicit trust

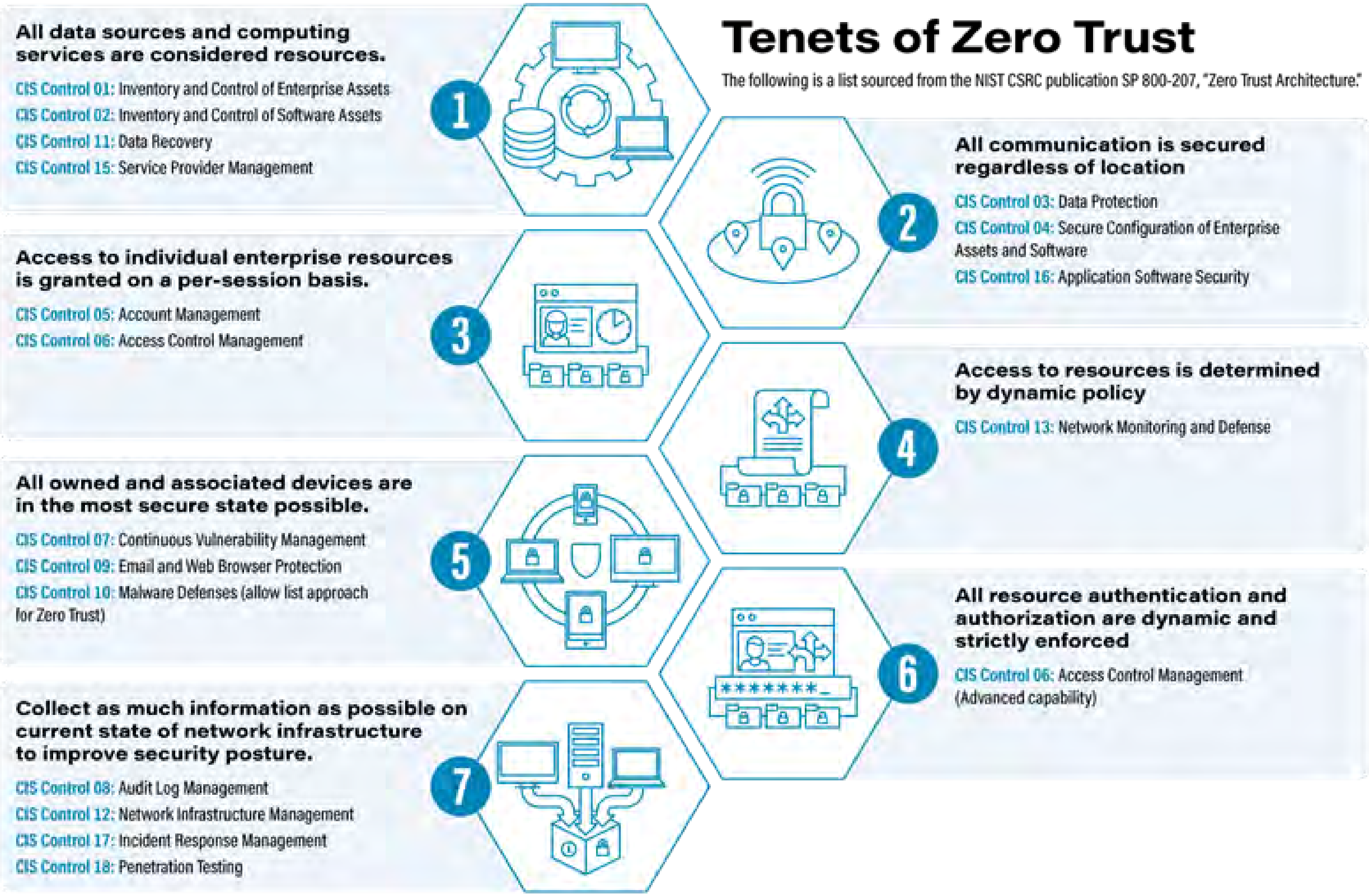
- Make this a risk-based decision
- Do NOT make the mistake of believing that you MUST go to FULL Zero Trust

First Steps

- ✓ Get information from your existing infrastructure and cybersecurity vendors as to how their hardware, software, or services may be configured and repositioned for a ZT architecture evolutionary path
- ✓ Use a mapping from the cybersecurity framework to Zero Trust
- ✓ Adopt a Zero Trust Maturity Journey option
- ✓ Continue the overall Security Journey

If you need assistance, engage a cybersecurity consultant.

Mapping: CIS to ZT Tenets



Tenets of Zero Trust

The following is a list sourced from the NIST CSRC publication SP 800-207, "Zero Trust Architecture."

1 All data sources and computing services are considered resources.

CIS Control 01: Inventory and Control of Enterprise Assets
CIS Control 02: Inventory and Control of Software Assets
CIS Control 11: Data Recovery
CIS Control 15: Service Provider Management

2 All communication is secured regardless of location

CIS Control 03: Data Protection
CIS Control 04: Secure Configuration of Enterprise Assets and Software
CIS Control 16: Application Software Security

3 Access to individual enterprise resources is granted on a per-session basis.

CIS Control 05: Account Management
CIS Control 06: Access Control Management

4 Access to resources is determined by dynamic policy

CIS Control 13: Network Monitoring and Defense

5 All owned and associated devices are in the most secure state possible.

CIS Control 07: Continuous Vulnerability Management
CIS Control 09: Email and Web Browser Protection
CIS Control 10: Malware Defenses (allow list approach for Zero Trust)

6 All resource authentication and authorization are dynamic and strictly enforced

CIS Control 06: Access Control Management (Advanced capability)

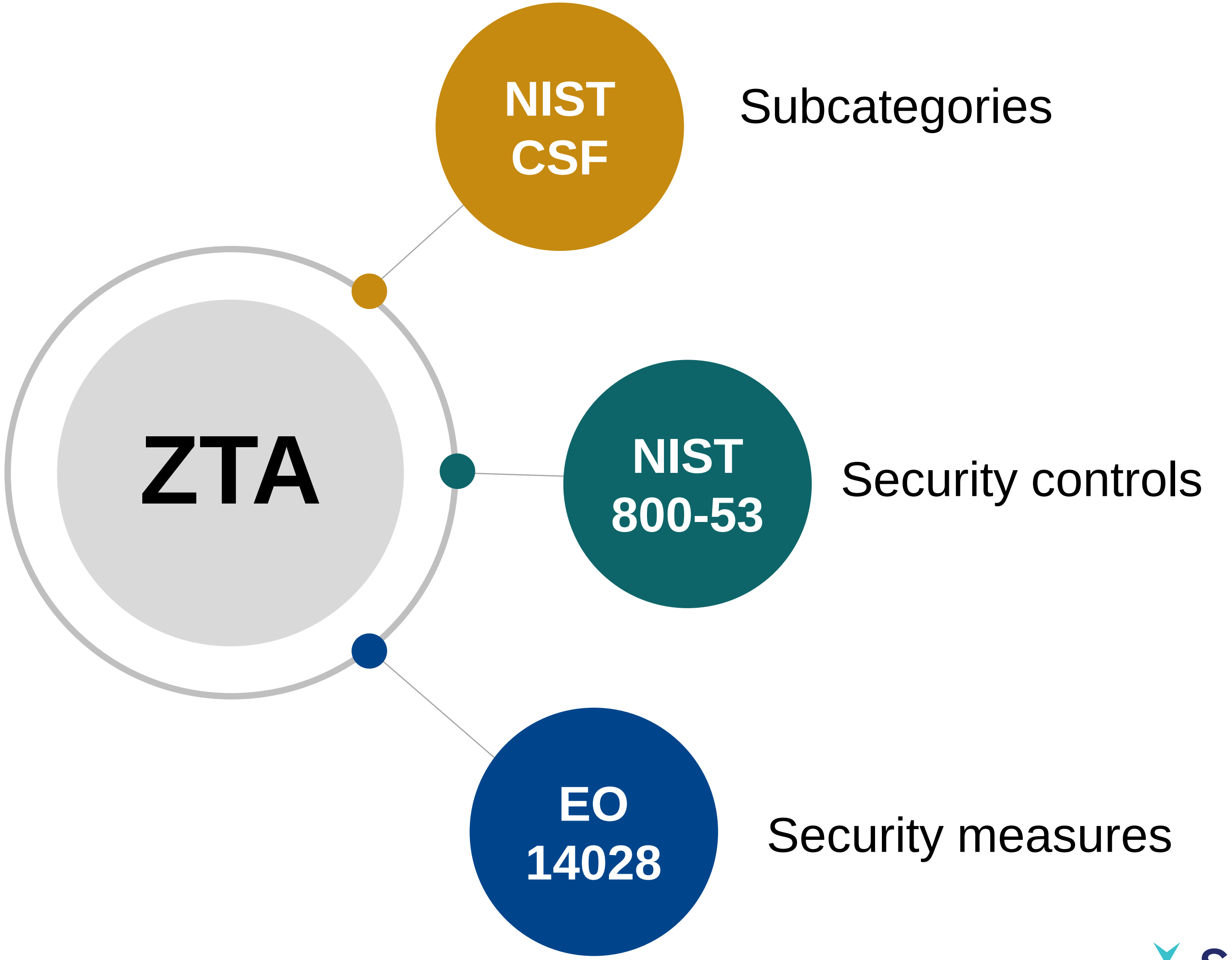
7 Collect as much information as possible on current state of network infrastructure to improve security posture.

CIS Control 08: Audit Log Management
CIS Control 12: Network Infrastructure Management
CIS Control 17: Incident Response Management
CIS Control 18: Penetration Testing

Mapping: NIST CSF/800-53 to ZTA

NIST National Cybersecurity Center of Excellence

- NIST SP 1800-35e: *Implementing a Zero Trust Architecture*



Key Takeaways

Balance

Compulsion

Way Forward

Balance

The key above all else is to establish a balance

- An acceptable compromise between enterprise security, system performance, and application usability
- A negotiated state that supports all stakeholders needs
- An environmental steady-state that is sustainable
- A solution that is supportable with the resources currently available and projected to be available over time

Not Compulsory

Unless you are a Federal or DoD entity

Not mandated as a statutory or regulatory obligation

Not mandated by any “Traditional” cybersecurity framework

Way Forward

Your current cybersecurity posture must be assessed against the appropriate cybersecurity framework and then mapped to your chosen ZT Journey

ZT Journey

- Everyone is doing it differently
- There is no one right path
- Advice: use the CISA Maturity Model for your ZT Journey
- Advice: review the DoD ZT Reference Architecture as an example infrastructure target
- Adapt both according to your needs and resources

Questions?

Thank You

Cameron Matthews

vCISO, Nth Generation

cameron.matthews@nth.com
619.384.8520

Multiemployer IT Summit

What's NExT?

AI: Meet Your Modern-Day Assistant

Christina "CK" Kerley, Technology Speaker, Trainer & Instructor

October 10-11, 2023 / San Diego

Proudly sponsored by

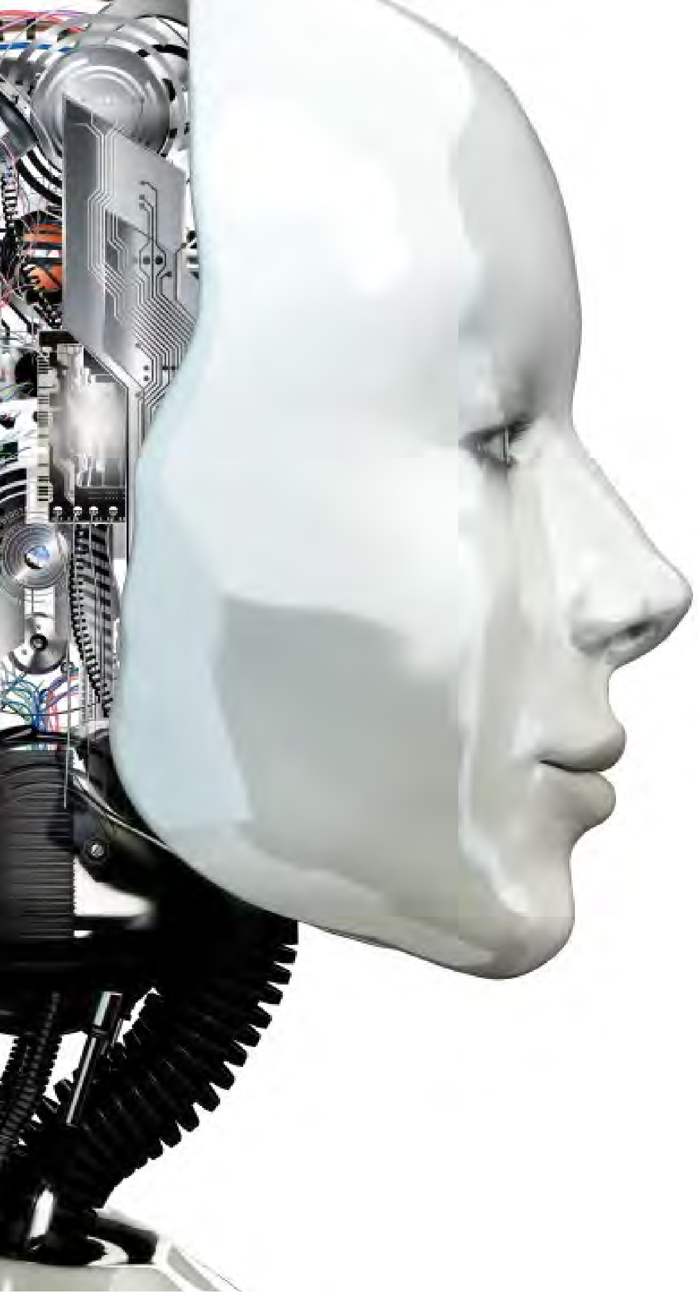
Segal

AI:

Meet Your Modern-Day Assistant

Christina "CK" Kerley

https://allthingsCK.com



We Are Moving From Working

ON

Machines . . .

To Working

WITH

Intelligent Machines

We Are Witnessing An Historic Paradigm Shift

1

What Is AI's Purpose In A Human-Dominated World?

2

What Is Humanity's Role In An AI-Centric Future?

3

Where Are Humans + Machines Headed Next?

AI Generates A Lot Of BIG Questions

“What Is AI’s Purpose In A Human-Dominated World?”

AI’s True Purpose In The Modern World:

To Assist And Elevate Humans In Their Work . . .

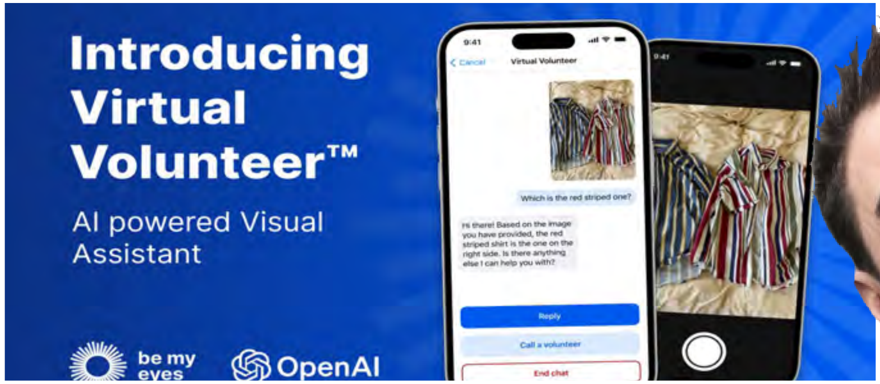
And Improve The Quality Of Their Lives

AIs Will Be Our Assistants, Coworkers & Collaborators

Personally, AIs Will Assist Us In Every Way That We Can Imagine

Providing Every Kid With An On-The Spot Tutor

Preventing Wildfires Get Out Of Control



Introducing Virtual Volunteer™

AI powered Visual Assistant

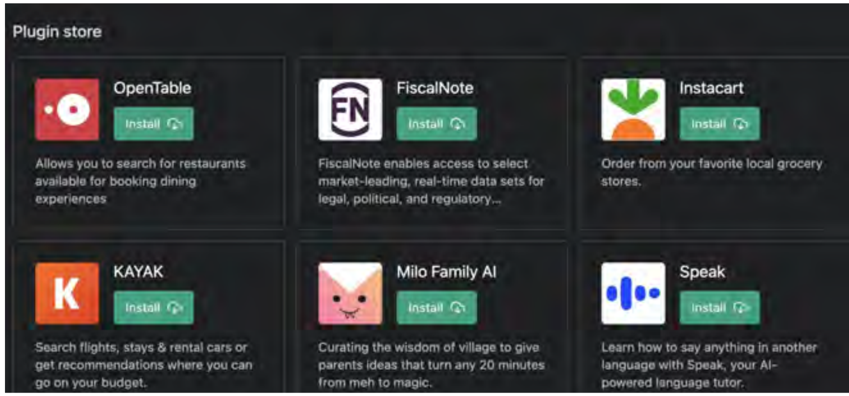
9:41

‹ Cancel Virtual Volunteer

Which is the red striped one?

Hi there! Based on the image you have provided, the red striped shirt is the one on the right side. Is there anything else I can help you with?

Help The Disabled Navigate The World



Plugin store

OpenTable

Install

Allows you to search for restaurants available for booking dining experiences

FiscalNote

Install

FiscalNote enables access to select market-leading, real-time data sets for legal, political, and regulatory...

Instacart

Install

Order from your favorite local grocery stores.

KAYAK

Install

Search flights, stays & rental cars or get recommendations where you can go on your budget.

Milo Family AI

Install

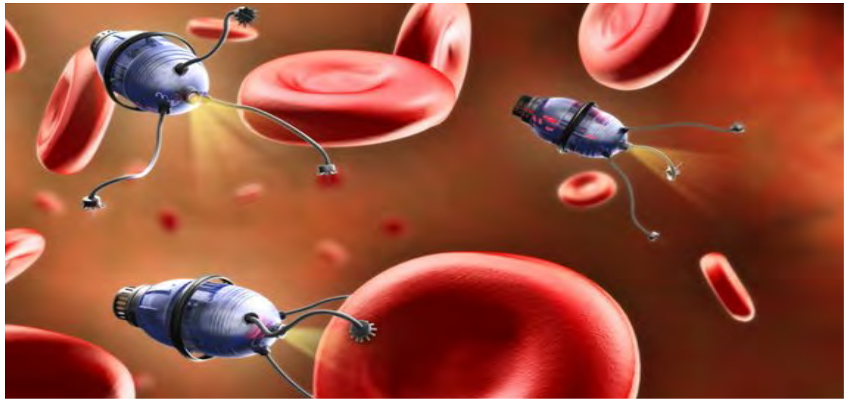
Curating the wisdom of village to give parents ideas that turn any 20 minutes from meh to magic.

Speak

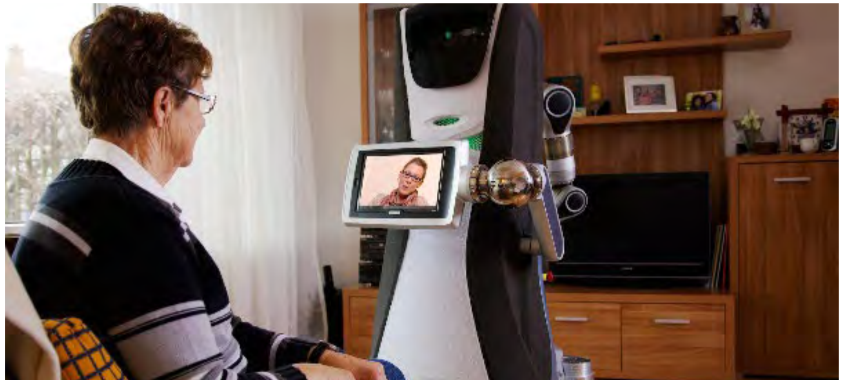
Install

Learn how to say anything in another language with Speak, your AI-powered language tutor.

Evolving The Web From Answers To Actions



Preventing Disease From Taking Hold



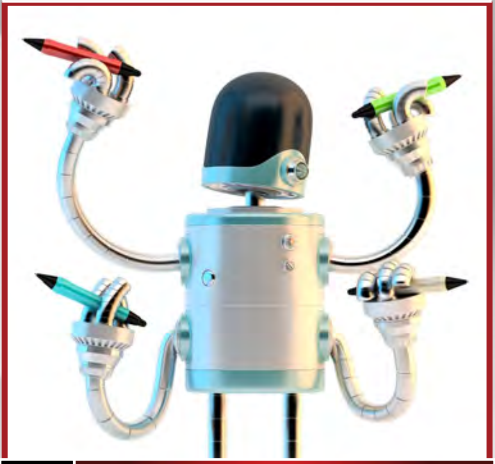
Enabling The Elderly To Live Freely

AI

Meet Your Modern-Day Assistant

Professionally, AI Will Assist Us In Many Ways . . . Through Many "Roles"

Assisting You Creatively



1 Creative Companion

Assisting You Administratively

2 Productivity Partner

Assisting You Promotionally

3 Customer-Interactions Sidekick

Assisting You Strategically

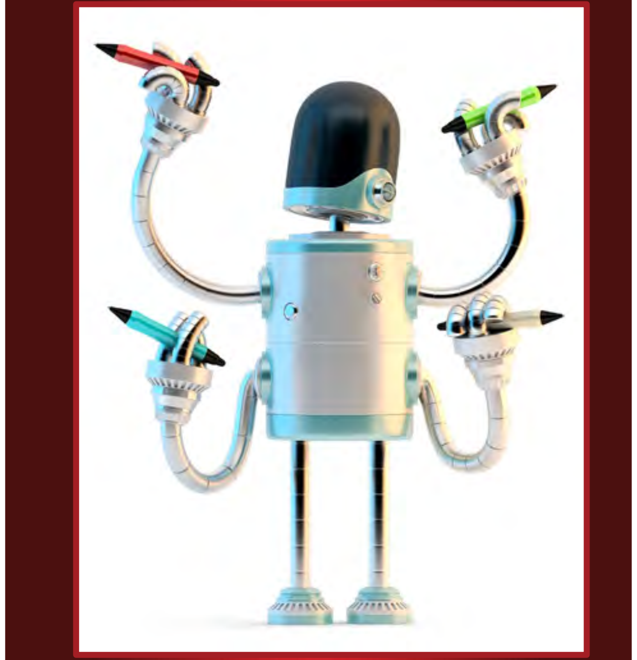
4 Innovation Guru

Assisting You Creatively

Assisting You By Enriching And Facilitating The Creative Process—Across Concepts, Writing, Editing, Design, And More!

Results are a function of:
(1) Data That AI systems are trained upon, (2) tools employed in the process and (3) Human oversight of all plans and programs

Modern-Day Assistant



Creative Companion

- Idea Generation
- Generating art, music, designs
- Writing & Editing
- Interactive Experiences
- Design Assistance
- Localization & Translation
- Mood & Tone Setting
- More!

Assisting You Administratively

Assisting You By Supporting, Streamlining, And Managing Tasks To Help You Maximize Every Moment Of Your Time!

Results are a function of:
(1) Data That AI systems are trained upon, (2) tools employed in the process and (3) Human oversight of all plans and programs

Modern-Day Assistant

Productivity Partner

- Automating repetitive tasks
- Scheduling and time management
- Assisting with task prioritization
- Integrating with productivity apps and tools
- Reminding about tasks and deadlines
- Summarizing content

Assisting You Promotionally

Assisting You Through Front-Line Customer-Service Help . . . And By Supporting Customer-Service Representatives!

Results are a function of:
(1) Data That AI systems are trained upon, (2) tools employed in the process and (3) Human oversight of all plans and programs

Modern-Day Assistant

Customer-Interactions Sidekick

- Answering FAQs instantly
- Handling complaints and feedback
- Automating routine support tasks
- Escalating complex issues to human agents
- Personalizing customer interactions based on data
- Analyzing customer feedback for insights

Assisting You Strategically

Assisting You As
A Key Resource For
Brainstorming,
Concepting, And
Improving:
Ideas, Strategies,
Prototypes, Plans,
And More!

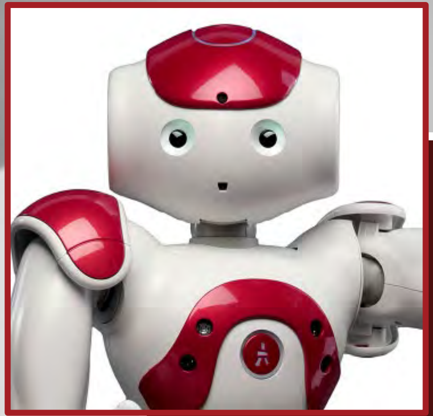
Modern-Day Assistant

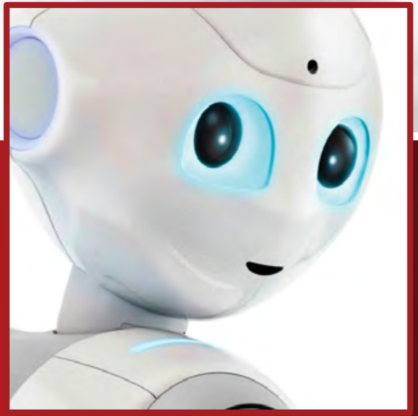
Innovation Guru

- Strategies
- Concepts
- Brainstorms
- Prototypes
- Discoveries
- Optimizations
- Simulations
- Models
- Modules

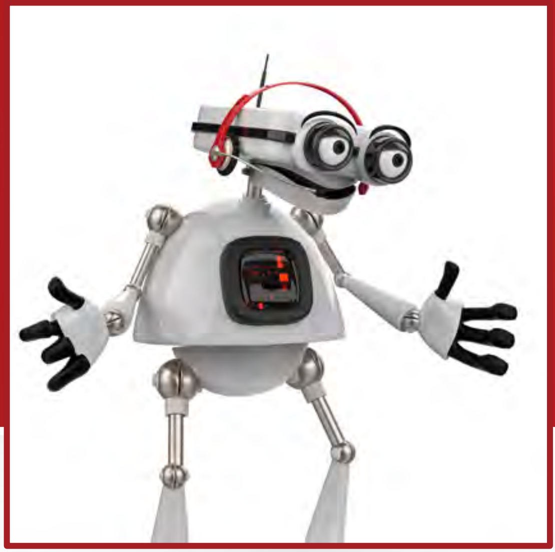
Results are a function of:
(1) Data That AI systems are trained upon, (2) tools employed in the process and (3) Human oversight of all plans and programs

“What Is Humanity’s Role In An AI-Centric Future?”





While The World Fixates On “The Rise Of The Robots” Another Extraordinary Phenomenon Is Emerging . . .



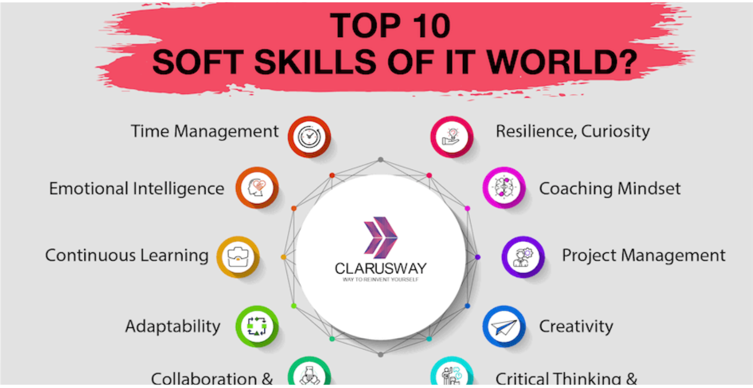
The Robots Give Rise To:

THE HUMAN RENAISSANCE

| Human-Centric Skills | Human Talent Shortage | Human-Centric Experiences | Human Expectations |

AI HERALDS A HUMAN FUTURE

1 HUMAN Skills



TOP 10 SOFT SKILLS OF IT WORLD?

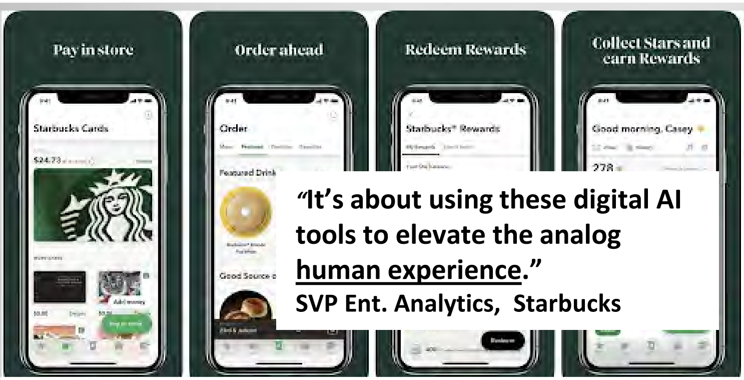
- Time Management
- Emotional Intelligence
- Continuous Learning
- Adaptability
- Collaboration &
- Resilience, Curiosity
- Coaching Mindset
- Project Management
- Creativity
- Critical Thinking &

AI Flips The Script:
Today's Soft Skills Will Be The Hard Skills Of Tomorrow

2 HUMAN Talent

The Future Of Work Is VERY Human:
85 Million Unfilled Jobs—$8-$15 Trillion In Lost Revenue

3 HUMAN Experience



"It's about using these digital AI tools to elevate the analog <u>human experience</u>."
SVP Ent. Analytics, Starbucks

Better Human-To-Machine Partnerships:
Make For Better Human-To-Human Experiences!

4 HUMAN Expectations

Hyper-Personalized Everything:
First We Shape Our Tools—Then Our Tools Shape Us

Driving

4 YEARS

OF YOUR LIFE

Waiting In Line

6 MONTHS

OF YOUR LIFE

Waiting On Hold

1.5 MONTHS

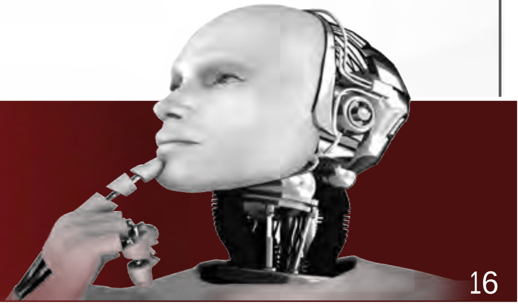
OF YOUR LIFE

Doing Chores

4-6 YEARS

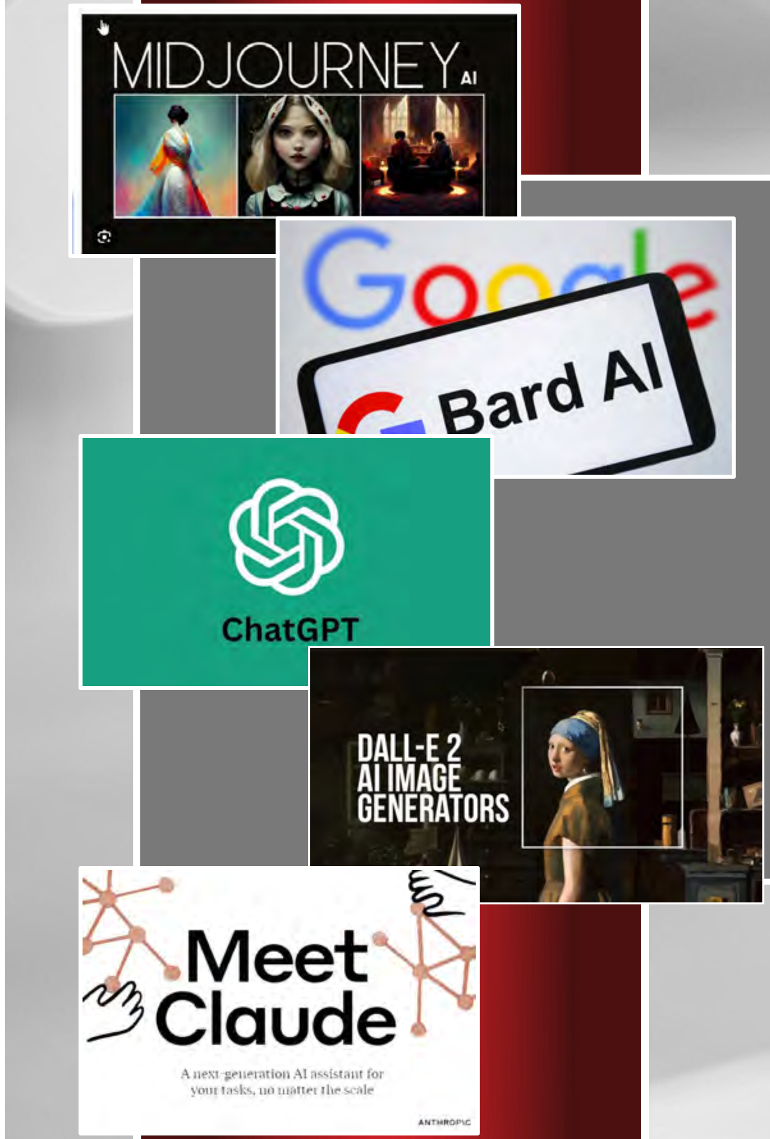
OF YOUR LIFE

More Time To Spend On The Projects, Passions,
And People That We Value The Most



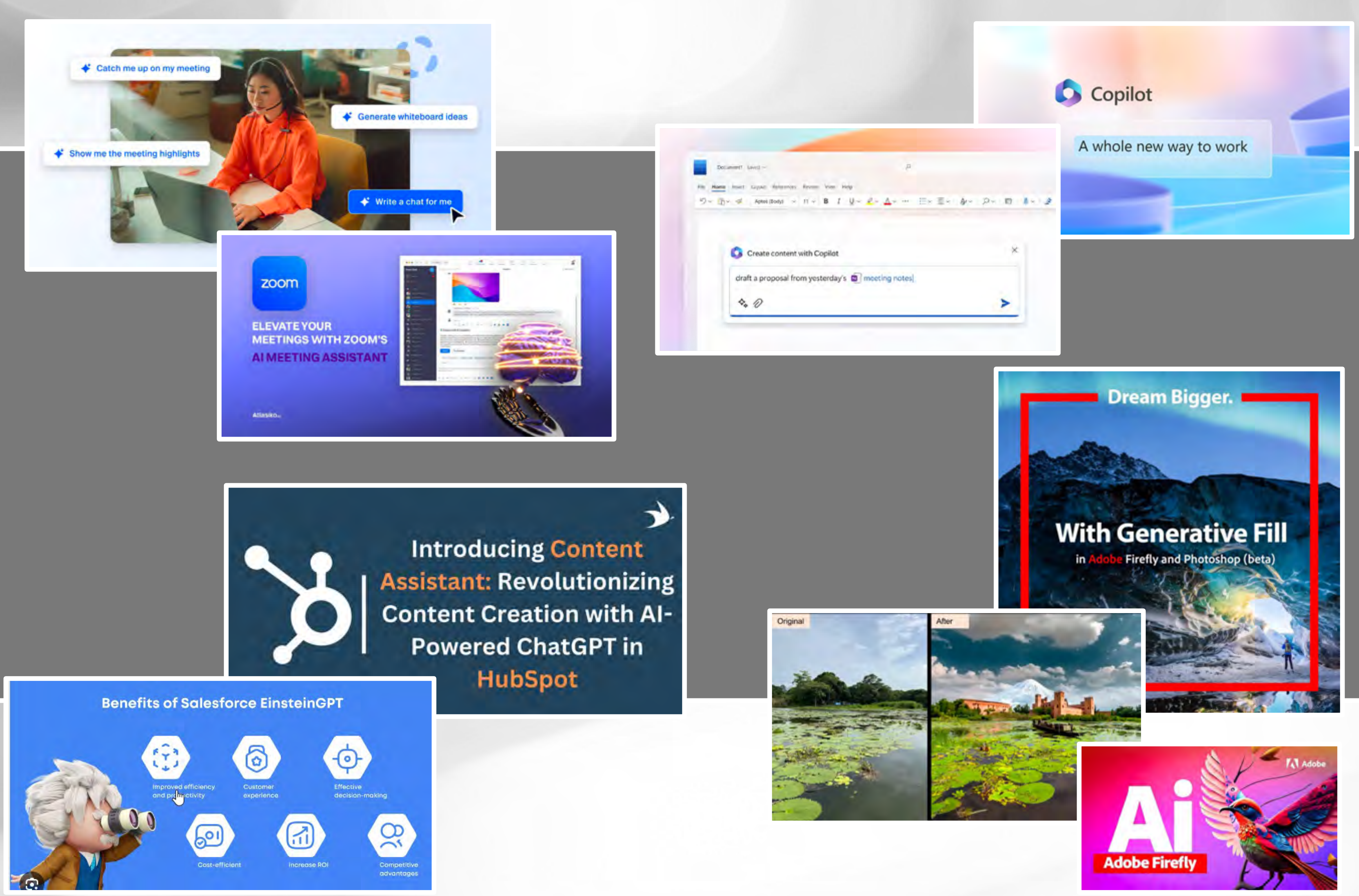
“Where Are Humans+ Machines Headed Next?”

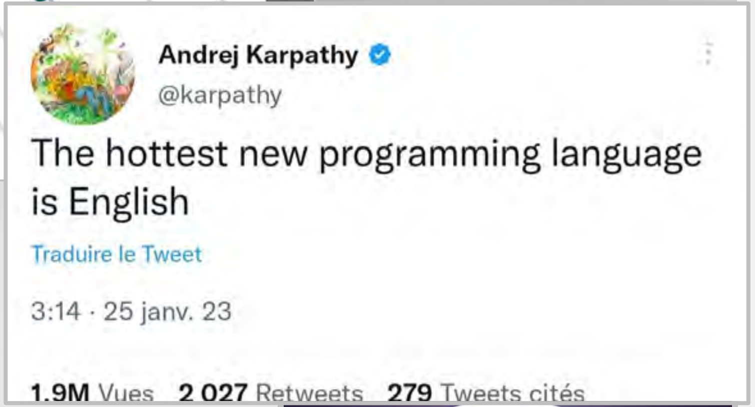
Individual AI Tools



AI Tools Will Become More Embedded Into Workflows

Instead of Taking Us Out Of The Moment—They'll Be Part Of All Moments/Devices


Catch me up on my meeting
Generate whiteboard ideas
Show me the meeting highlights
Write a chat for me
zoom
ELEVATE YOUR MEETINGS WITH ZOOM'S AI MEETING ASSISTANT
Copilot
A whole new way to work
Create content with Copilot
draft a proposal from yesterday's meeting notes
Introducing Content Assistant: Revolutionizing Content Creation with AI-Powered ChatGPT in HubSpot
Benefits of Salesforce EinsteinGPT
Improved efficiency and productivity
Customer experience
Effective decision-making
Cost-efficient
Increase ROI
Competitive advantages
Dream Bigger.
With Generative Fill
in Adobe Firefly and Photoshop (beta)
Original
After
Adobe
Ai
Adobe Firefly

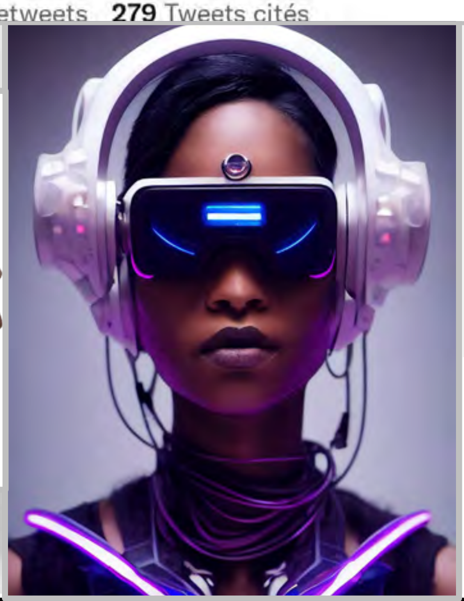

Andrej Karpathy
@karpathy

The hottest new programming language is English

Traduire le Tweet

3:14 · 25 janv. 23

1.9M Vues 2 027 Retweets 279 Tweets cités



Instead Of Us Constantly

Technology Finally Focuses ON US!

FIXATED On Technology

| Tech Gets Easier | Smartphones Get Smarter | The Web Gets "Human" | Benefits Are Immediate | More AI-First Devices |

From Reactive “Sick Care”. . .

Re-vamped Care Model

PREVENTATIVE Healthcare

To Preventative Health Care

From Generalized Learning . . .

Re-invented Learning Model

PERSONALIZED Education

To Personalized Learning

From Wasteful Systems . . .

Re-imagined Agriculture Model

PRECISION Agriculture

To Precision Agriculture

As AIs Get Smarter—Humans Keep Getting Wiser, Too!

40% Of Employees Require Reskilling Over Next 3 Years

IBM

50% Of Employees Require Reskilling By 2025

World Economic Forum

$15 Trillion In Revenue At Stake

1.4 Billion Of The 3.4 Billion In The Global Workforce

World Bank

Up To 90% Of Employees Will Need Reskilling By 2030

World Economic Forum

AI’s True Purpose In The Modern World:

To Assist And Elevate Humans In Their Work . . .

And Improve The Quality Of Their Lives

AIs Will Be Our Assistants, Coworkers & Collaborators

“Thank
YOU
So Much!”

Christina “CK” Kerley
https://allthingsCK.com

Multiemployer IT Summit

What's NExT?

Compliance Update for Retirement and Health Funds along with HIPAA Security and DOL Cybersecurity Review

Michael Stoyanovich, VP and Senior Consultant, Segal's Administration & Technology Consulting Practice

Kristina Zinnen, JD, VP and Senior Consultant, National Retirement Compliance Practice, Segal

October 10-11, 2023 / San Diego

Proudly sponsored by

Segal

Agenda: Retirement

1. SECURE 2.0
2. PBGC Regulations
3. Fiduciary Duty

SECURE 2.0

SECURE 2.0

Background

- SECURE 2.0 Act of 2022 was enacted December 29, 2022 as part of the 2023 Consolidated Appropriations Act
- The law contains more than 90 provisions, with different effective dates
- Most provisions have delayed effective dates to plan years beginning on or after January 1, 2024, or later; we will focus on the 2023 provisions
- Plans must comply operationally based on the applicable effective date
  - No written amendments are required before the end of the 2025 plan year (end of 2027 plan year for collectively bargained and government plans)

SECURE 2.0

Increase the Required Beginning Date Age (RBD)

- SECURE Act of 2019 increased RBD age from 70½ to 72
- Increases RBD age to 73 for anyone who had not attained age 72 before January 1, 2023
- Increases RBD age to 75 for anyone who had not attained age 74 before January 1, 2033
- This is a change to the tax rules that does not affect when plans can require participants to begin receiving benefits

SECURE 2.0

Other Required Minimum Distribution (RMD) provisions

- Reduce penalty for RMD failures
  - Reduces the penalty tax on participants who fail to take RMDs from 50% to 25% of the missed distribution; further reduced to 10% if corrected timely (~2 years)
- Partial lump sum, partial annuity
  - When an RMD is partially from an annuity and partially from the balance of the account, the RMD from the total account is reduced by the amount of the annuity payment
- Allow surviving spouse to elect to be treated as the employee
  - Allows the surviving spouse of a participant who dies before RBD to elect a more favorable life expectancy table (the uniform life table) for the spouse's beneficiary

SECURE 2.0

Corrections

- No requirement to recover plan overpayments
  - Plan fiduciaries would not be required to seek recovery of mistaken overpayments from participants when participant is not at fault for the overpayment
- Limitations if pursuing recovery of overpayments
  - Fiduciaries’ ability to recover overpayments limited if "inadvertent error" first occurred more than 3 years before resulting overpayment was identified
  - Plan is not allowed to charge interest
  - Reductions are limited to 10% of correct payment amount
  - Fiduciaries may consider the participant’s financial hardship

SECURE 2.0

Corrections

- Self-correction
  - Broadly expands a plan’s ability to use self-correction if the failure is inadvertent
  - Relief from DOL rules for failures related to loans
  - Treasury is to revise Employee Plan Compliance Resolution System (EPCRS) guidance no later than December 29, 2024
  - IRS Notice 2023-43 confirms that plans can use this relief prior to the issuance by IRS of revised EPCRS guidance – including failures predating December 29, 2022 that have not been corrected

SECURE 2.0

New Exceptions to Early Withdrawal Penalty

- Withdrawals related to domestic abuse
  - Special distribution due to domestic abuse exempt from 10% premature distribution penalty
  - Must satisfy domestic abuse standard of IRC § 72
  - Limited to $10,000 or 50% of the account, if less; may be repaid to an IRA (or plan may accept repayments) within three years
- Terminally ill individuals
  - 10% early withdrawal penalty no longer applies in the case of distribution to a terminally ill participant (after doctor certification); amounts may be repaid within 3 years

SECURE 2.0

New Exceptions to Early Withdrawal Penalty

- Substantially equal periodic payments
  - SECURE 2.0 clarifies that the exception continues to apply after rollover, exchange of nonqualified annuities, or RMD
- Federally declared disasters
  - SECURE 2.0 provides permanent rules for the use of retirement funds in any federally declared disaster
  - DC plans can permit distributions of up to $22,000 free of the 10% premature distribution penalty; participant can spread the income over three years for federal income tax purposes
  - The plan could be amended to include the automatic disaster trigger

SECURE 2.0

New Exceptions to Early Withdrawal Penalty

- Qualified birth or adoption distribution repayments limited to three years from the distribution date
  - Only relevant for a plan that specifically addresses birth and adoption distributions and allows them to be rolled back into the plan
  - Plan must be amended to limit rollover to within three years for amounts withdrawn after enactment (and to January 1, 2026, for earlier distributions)
- Self-certification of safe-harbor hardship event
  - Plans may allow participants to self-certify any component of hardship eligibility, including financial need; forthcoming guidance may provide that plan cannot accept self-certification if it has actual knowledge of falsehood

SECURE 2.0

Native American tribal court QDROs

- Plans are required to treat domestic relations orders issued by Native American Tribal Courts in a manner similar to those issued by other courts
- Effective for domestic relations orders received by the plan after December 31, 2022, including any such order which is submitted for reconsideration after such date
- Because of the statutory language, there has been a question whether domestic relations orders issued by a Native American Tribal Court can be QDROs

SECURE 2.0

Other optional changes effective in 2023

- Qualifying Longevity Annuity Contract (QLAC) limitations eased
- Commercial annuity provisions broadened (only applies to commercial annuities purchased by plan)
- Mixed-performance benchmarks permitted for investments
- Unenrolled participants need not receive some notices (optional)
- Rule for correcting automatic enrollment failures extended
- Small immediate financial incentives to employee for elective contribution allowed

PBGC Regulations

PBGC Regulations

PBGC Final Rule on Multiemployer Special Financial Assistance (SFA)

- Two-interest rate approach: one for non-SFA assets and one for SFA assets
  - Most eligible plans will receive a greater amount of SFA because of the lower interest rate for SFA assets
- Broadened SFA investment options
  - Up to 33% in “return-seeking investments”
  - Remainder in investment-grade fixed income

PBGC Regulations

PBGC Final Rule on Multiemployer Special Financial Assistance

- New methodology for Multiemployer Pension Reform Act (MPRA) plans
- Withdrawal liability
  - Mass withdrawal liability interest rates used until the later of 10 years or the projected life of the SFA assets
  - Phase-in recognition of SFA assets
- Mergers involving SFA-recipient plans
  - Requires PBGC approval but the merged plan may seek a waiver of certain conditions from the PBGC

PBGC Regulations

PBGC Final Rule on Multiemployer Special Financial Assistance

- SFA measurement date and “lock-in” applications
  - Base data (e.g., interest rate and census data) is measured from the last day of the third calendar month immediately preceding the plan’s initial application
  - Plans may file a “lock-in application” through 2025, even if the PBGC temporarily closes its filing portal, to allow plans to file using a specific measurement date
- Supplemental filings
  - Plans that have been approved can submit a supplemental filing to increase SFA amounts due to updated provisions in the final rule

PBGC Regulations

PBGC Proposed Rule on Actuarial Assumptions

- ERISA § 4213 provides employer assessed withdrawal liability determined on basis of:
  - Reasonable actuarial assumptions and methods, reflecting…the actuary’s best estimate of experience under the plan; or
  - Actuarial assumptions and methods as set forth in PBGC regulations
- PBGC released proposed rule on October 14, 2022
  - Provides an acceptable range of interest rates used to calculate withdrawal liability from PBGC annuity rates to funding rates
  - Segal Blend falls within the acceptable range
- Comments were due to PBGC December 13, 2022, awaiting final rule

Fiduciary Duty

Fiduciary Duty

DOL Final Rule: Prudence and Loyalty in Selecting Plan Investments and Exercising Shareholder Rights

- Fiduciaries may treat environmental, social and governance (ESG) factors as directly related to risk and reward opportunity
  - Recently upheld in *Utah v. Walsh* (ND Texas)
- ESG-focused investment options may be used as a plan's qualified default investment alternative (QDIA)
- Fiduciaries may consider collateral benefits
  - As tiebreakers between economically indistinguishable investments
  - When constructing a menu of prudent investment options for participant-directed individual accounts

Fiduciary Duty

DOL Proposed Rule on Conflict of Interest in Investment Advice – Coming Soon!

- New version of the proposed fiduciary rule sent to OMB on September 8, 2023, expected to be released in October
- Rule would "more appropriately define when persons who render investment advice for a fee to employee benefit plans and IRAs are fiduciaries" within the meaning of ERISA and the Internal Revenue Code

Agenda: Health

1. **Mental Health Parity and Addiction Equity Act (MHPAEA)**
2. **Inflation Reduction Act**
3. **No Surprises Act/Transparency in Coverage**
4. **ACA Preventive Services**
5. **Post-*Dobbs***
6. **PBM Reform Legislation**

Mental Health Parity and Addiction Equity Act (MHPAEA)

Mental Health Parity & Addiction Equity Act

Background on MHPAEA

- 2013 Final Regulations
  - MHPAEA requires parity between medical/surgical (med/surg) benefits and mental health (MH) and substance use disorder (SUD) benefits
  - 2013 final regulations set out parity standards in the following areas:
    - Quantitative parity analysis (financial requirements & treatment limits)
    - Parity with respect to non-quantitative treatment limits (e.g., medical management)
    - Certain designs specifically prohibited (e.g., separate deductibles or out-of-pocket limits)
  - No requirement to provide MH or SUD coverage (but IF covered, must cover in every classifications where med/surg services are provided)

Mental Health Parity & Addiction Equity Act

Background on MHPAEA

- 2021 Consolidated Appropriations Act
  - Requires group health plans to perform and document comparative analyses of the design and application of nonquantitative treatment limitations (NQTLs) in six classifications, and perform a corrective process if out of compliance
    - Examples of NQTLs: prior authorization, exclusion of specific treatments for certain conditions, restrictions on provider billing codes, methods for determining usual, customary, and reasonable charges
  - Plans were required to be prepared to make these comparative analyses available to the DOL and/or HHS upon request
  - Plans generally have been working with benefit administrators to collect documented NQTL comparative analyses regarding administrative activities

Mental Health Parity & Addiction Equity Act

Background on MHPAEA

- Federal enforcement has continued to increase
- Plan changes following DOL investigations include removal of:
  - Exclusions for applied behavioral therapy to treat autism
  - Exclusions for medication-assisted treatment for opioid disorder
  - Nutrition counseling exclusions if more restrictive for mental health conditions (e.g., anorexia) than medical condition (e.g., diabetes)
  - Residential treatment exclusions
  - Blanket prior authorization requirements

Mental Health Parity & Addiction Equity Act

MHPAEA Proposed Regulations

- On July 25, 2023, the Departments issued a package:
  - Proposed rules, later formally published in the FR on August 3
  - Technical release seeking information and comments with respect to guidance for proposed data collection and evaluation requirements for nonquantitative treatment limitations related to network composition
  - The 2023 MHPAEA Comparative Analysis Report to Congress
  - Enforcement Fact Sheet regarding fiscal year 2022 enforcement results
  - Press Release announcing guidance

Mental Health Parity & Addiction Equity Act

MHPAEA Proposed Regulations

- The August 3, 2023, proposed rules revise the 2013 final rules as well as including new, additional requirements related to documented NQTL comparative analyses
- Proposed applicability for plan years beginning on and after January 1, 2025

Mental Health Parity & Addiction Equity Act

MHPAEA Proposed Regulations

- Includes changes to the 2013 MHPAEA final regulations as well as new, additional requirements, including required data collection
- Includes new provisions for the content requirements of the NQTL comparative analyses required under MHPAEA.
- Provides transition period to comply with new requirements. Proposes plan years beginning on or after January 1, 2025 applicability date.
- Includes HHS-only amendments to implement the sunset provision for self-funded, non-Federal governmental plan elections to opt out of compliance with MHPAEA

Mental Health Parity & Addiction Equity Act

MHPAEA Proposed Regulations Include

- Revised,expanded list of NQTLs
- Network composition NQTLs
- NQTLs listed in the preamble
- New 3-part test for the application of NQTLs
- Expanded data collection requirements
- Network composition NQTLs data
- Proposed enforcement safe harbor

Inflation Reduction Act of 2022

Inflation Reduction Act

Background

- Enacted August 16, 2022, the Act significantly changes Medicare coverage
  - Medicare will negotiate prices for certain prescription drugs
  - Medicare will receive inflation rebates from manufacturers
  - Part D coverage changes significantly
  - Additional Medicare coverage for vaccines and insulin

Inflation Reduction Act

Insulin coverage

- Medicare changes
  - During plan years 2023, 2024, and 2025: Medicare beneficiaries cannot be required to pay more than $35 for a 30-day supply of insulin
- HSA/HDHP changes
  - In 2023 and thereafter, HSA-qualified HDHPs may cover insulin before the deductible is met
- The cap on insulin copayments does not apply to group health plans or employer-sponsored plans
  - The cap also does not apply to a retiree plan that gets the Retiree Drug Subsidy

Inflation Reduction Act

Part D benefit changes

- Medicare Part D coverage significantly modified to eliminate participant coinsurance during the catastrophic payment period, and change who pays during that period
- By 2025, annual out-of-pocket maximum of $2,000 (smoothing permitted to allow beneficiaries to pay monthly)
- Part D premiums: increases limited to six percent per year from 2024–2029 (note: many are doubling from 2023 to 2024)
- Manufacturer discount program changed
- Expanded income eligibility for Low Income Subsidy

Inflation Reduction Act

Medicare negotiations

- On August 29, 2023, CMS announced the first 10 drugs covered by Medicare Part D selected for negotiation
  - Chosen from list of 50 highest-spending, brand-name drugs covered by Medicare Part D
  - Negotiated prices will be available starting in 2026
- Medicare will choose and negotiate 15 more Part D drugs for 2027, 15 more Part B or Part D drugs for 2028, and 20 more Part B or Part D drugs for each year after that

No Surprises Act / Transparency in Coverage

No Surprises Act / Transparency in Coverage

Background

- Effective for plan years beginning on or after January 1, 2022
- Multiple regulatory initiatives
  - Gag clause attestation
  - Independent Dispute Resolution
- Awaiting guidance
  - Air ambulance data reporting
  - Advanced Explanation of Benefits (EOB) and Good Faith Estimate

No Surprises Act / Transparency in Coverage

Gag clause prohibition under the NSA

- Effective December 27, 2020, health plans and insurance issuers may not enter into contracts that would restrict the plan from:
  - Disclosing provider-specific cost or quality of care information
  - Electronically accessing de-identified claims and encounter information or data consistent with HIPAA, GINA, and ADA
  - Sharing this information data/data with a business associate
- Plans must complete attestation that they do (or did) not have gag clauses in contracts by December 31, 2023

No Surprises Act / Transparency in Coverage

Independent Dispute Resolution process

1

The Qualifying Payment Amount (QPA) must be used to calculate **participant cost-sharing** for Emergency Services at an Out-of-Network provider or facility, Non-Emergency Services at certain In-Network Facilities, and Non-Network Air Ambulance Services

2

If the plan sends the provider/facility an **initial payment or notice of denial**, it must tell them what the QPA is for that service

3

IDR **MUST** consider: QPA; quality and outcomes measurements of the provider/facility; market share; complexity of case; teaching status, case mix, and scope of services of facility; good faith efforts to enter into network agreements; additional credible information

MAY NOT consider: UCR, billed amount, public payer rates

No Surprises Act / Transparency in Coverage

Independent Dispute Resolution process

- U.S. District Court for the Eastern District of Texas issued a judgment and order vacating certain portions of the Departments' August 2022 final rules and related guidance
- IDR is paused pending further guidance from HHS
  - Proposed regulations issued last week
- IDR process is backlogged
  - Between April 15, 2022, and March 31, 2023, 334,828 disputes initiated through the IDR Portal
  - 14x more than expected; party initiating IDR (usually the providers) prevailed in 71% of disputes

Affordable Care Act (ACA) Preventive Services

ACA Preventive Services

Background

- The ACA's preventive services mandate requires non-grandfathered group health plans and insurers to cover certain preventive services with no cost sharing on an in-network basis

ACA Preventive Services

ACA preventive services litigation

- On March 30, 2023, the U.S. District Court for the Northern District of Texas ruled that part of that mandate violates the Constitution violates the Constitution because members of the United States Preventive Services Task Force (USPSTF) have not been appointed in a manner consistent with Article II’s Appointments Clause
- The court ordered that the preventive care requirements issued based on the USPSTF are vacated and the federal government is enjoined from implementing or enforcing them
  - The court’s order does not appear to extend to ACA-mandated preventive care recommended by the ACIP or the HRSA, including contraceptive coverage and vaccines

ACA Preventive Services

ACA preventive services litigation

- Plan sponsors do not need to take any action in response to this decision and may be best served by monitoring the response by the federal government and higher courts
- FAQ 59:
  - "... the Departments strongly encourage plans and issuers to continue to cover such items and services without cost sharing. Preventive services help people avoid acute illness, identify and treat chronic conditions, reduce the risk of cancer or facilitate early detection, and improve health."

ACA Preventive Services

ACA preventive services litigation

- The Administration has appealed the decision, and the Fifth Circuit Court of Appeals issued a stay. Consequently, the preventive services requirements remain in place until further action from the courts
  - Provider groups agreed not to oppose agencies' motion to stay lower court's decision
  - Agencies agreed not to seek penalties or enforcement for periods before case is resolved
- Dozens of patient advocacy groups have asked to file amicus briefs in support of the ACA requirement, arguing that the decision will lead to an uptick in preventable deaths, especially among people who otherwise could not afford health care

Post-Dobbs v. Jackson Women’s Health Organization

Post-*Dobbs*

State of the states following Dobbs

- Approximately 16 states have some type of protection for abortion in place
- Abortion is currently illegal or heavily restricted in 17 states
- Some states have ongoing lawsuits over the interpretation and application of state law - six states currently have abortion bans on hold that were blocked by courts
- More bans expected as lawmakers in other states have proposed new laws to restrict abortion access

Post-*Dobbs*

ERISA preemption

- Generally, ERISA preempts state laws that relate to an employee benefit plan
- Consequently, self-insured group health plans can continue to design benefits without complying with state insurance law, but state insurance law would generally apply to fully-insured group health plans
- Criminal laws are not generally preempted by ERISA, but the issue will depend on how the law is written and applied
- ERISA preemption application in the state abortion law area has not yet been litigated

Post-*Dobbs*

Medication abortion litigation

- Texas District Court stayed the FDA’s 2000 approval of mifepristone
  - Washington District Court ruled in favor of 17 states and Washington, D.C., requiring FDA to keep mifepristone available in those jurisdictions
- Supreme Court issued a stay pending disposition of the appeal in the Fifth Circuit and the disposition of a writ of certiorari
- Fifth Circuit upheld FDA’s 2000 approval but rolled back 2016 and 2021 changes (ability to take drug at 10 weeks, mail order)
- Supreme Court appeal is expected; ruling does not affect current availability of mifepristone, pending Supreme Court’s final ruling

Post-*Dobbs*

Contraceptive coverage

- Affordable Care Act requires non-grandfathered group health plans and issuers to cover, without cost sharing, at least one form of contraceptive in each method for women currently identified by the U.S. Food and Drug Administration (FAQ 54)
  - Plans must have medical exceptions process stated clearly in SPD and available without having to make an appeal
  - Free coverage may be limited to in-network
  - Coverage includes Plan B (emergency contraceptives)
- Secretaries Walsh, Becerra, and Yellen have announced an enforcement initiative

Post-*Dobbs*

Executive Order on contraceptives and family planning

- Directs Treasury, Labor, and HHS to issue guidance to improve Americans’ ability to access low- or no-cost contraception
- Secretaries are directed to:
  - Ensure coverage of all contraceptives approved, granted or cleared by the FDA, without cost sharing
  - Streamline the process for patients and healthcare providers to request coverage, without cost sharing, of medically necessary contraception.
  - Promote increased access to affordable over-the-counter contraception, including emergency contraception.

Pharmacy Benefit Manager (PBM) Reform Legislation

PBM Reform Legislation

Lower Costs, More Transparency Act

- Introduced by the House Committees on Education & the Workforce, Energy & Commerce, and Ways & Means on September 8, 2023
  - Increases price transparency
  - Addresses prescription drug costs
  - Supports community health centers, health care workers
  - Increases access to health data and fees

PBM Reform Legislation

Senate Bill 1339, Pharmacy Benefit Manager Reform Act

- Reported by Senator Sanders to the Committee on Health, Education, Labor, and Pensions on June 22, 2023
  - PBMs must report annually to the plan sponsor certain information about the PBM’s services, including amount of copayment assistance funded by drug manufacturers, list of covered drugs billed under the plan during the reporting period, and total net spending by the health plan on prescription drugs
  - PBMs also must provide plan sponsors with a supplementary report every six months with specified information about drugs that dispensed under the plan by pharmacies wholly or partially owned by the PBM

Agenda – HIPAA Security Update

1. The OCR’s Bulletin Addressing Tracking Technologies
2. Uses and Misuses of Data Collected by Tracking Technologies
3. Your Next Steps
4. Enforcement
5. Breach Notifications and Class Action Lawsuits
6. Conclusion

Pixel Me Not

The Use of Tracking Technologies and the OCR’s Bulletin that will Change Your Life

(Well, At Least Your Web and Mobile Apps)

The OCR is Back!

- The HHS' Office for Civil Rights has issued a bulletin on 12/01/2022.
- The bulletin confirms that:
  - The use of third-party tracking technologies (aka pixels) on websites, web applications, and mobile apps without a business associate agreement (BAA) is a HIPAA violation if the tracking technology collects and transmits individually identifiable health information.
- You can read the complete bulleting following this link: Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates | HHS.gov

Tracking Technologies

- Definition
  - – Snippets of code applied to websites, web applications, and mobile apps to track user activity.
- The Good Intentions
  - – Data collected by these technologies helps covered entities analyze how to improve theirs services, boost user experience, therefore benefits patients.
- The Road to Hell
  - – Data collected through these technologies is usually transmitted to the tech vendor – for example, Meta or Google Analytics – which in turn, sends it to third parties.
  - – Tracking technologies can collect device-related information through which a user could be identified.

Impact

- Information disclosed in confidence by a patient using websites, web applications, or mobile apps can potentially be transferred to third parties, including law enforcement.
- Third parties may use data for any purpose:
  - From targeted ads to fraud, identity theft, extortion, stalking, harassment, or to misinform.

Your Next Steps

- Conduct an evaluation of tracking technologies used on your websites, web applications, and/or mobile apps to ensure those technologies are aligned with the HIPAA Privacy and Security Rules.
  - If the evaluation reveals tracking technologies are or were used in a manner not compliant with the HIPAA Rules, then the HIPAA Breach Notification Rule applies.
  - Notifications will need to be sent to OCR and the individuals whose PHI has been impermissibly disclosed.
- Include website tracking technologies in your next periodic risk assessment.
- Tracking technology vendors are business associates under HIPAA; make sure you have a BAA in place.

Covered Entities Already Reporting

Most Notable:

- January 2023: UCLA Health notified nearly 94,000 patients about an impermissible disclosure of their ePHI to certain unnamed service providers due to the use of analytics tools on its website and mobile app.
- March 2023: New York Presbyterian Hospital (NYP) has confirmed that tracking and analytics tools used on its website, nyp.org, which may have resulted in patient information being impermissibly disclosed to third-party service providers that developed the tools.

How Proactive is the OCR about Enforcement?

Slow and Trending Upwards

- Both the OCR and the Federal Trade Commission (FTC) have published letters that were sent to hospital systems and telehealth providers in July 2023.
- Letters advised entities about the privacy risks associated with website tracking technologies such as Meta Pixel and Google Analytics.
- The recipients of the letters were made public in document jointly published by OCR and FTC on their websites. You can ready the document here: ocr-ftc-letters-re-use-online-tracking-technologies.pdf (hhs.gov)
- While OCR and the FTC had reason to issue the letters to specific entities, receipt of a letter does not imply violations have been uncovered.

Case Study: Medtronic MiniMed and MiniMed Distribution Corp

- Lawsuit filed District Court for the Central District of California against Medtronic over the use of tracking technologies in its InPen diabetes management app – September 2023.
- Plaintiffs claim ePHI and confidential information was disclosed to third parties via Google Analytics, Firebase, and Crashlytics.
- Medtronic reported the data breach to the OCR in April as affecting 58,374 individuals.
- Email and IP addresses, phone numbers, InPen App usernames and passwords, timestamp information for InPen App events, and unique identifiers for InPen accounts or mobile devices were impermissibly disclosed.

Case Study: Medtronic MiniMed and MiniMed Distribution Corp

- The lawsuit alleges common law invasion of privacy – intrusion upon seclusion, breach of confidence, breach of fiduciary duty, negligence, breach of implied contract, breach of implied covenant and fair dealing, unjust enrichment, and violations of the Electronic Communications Privacy Act (ECPA), California Invasion of Privacy Act (CIPA), and New York General Business Law.
- The lawsuit seeks class action status, a jury trial, damages, extended credit monitoring services, attorneys' fees, and equitable and injunctive relief to ensure that users of its app have their privacy protected.

Other Notable Class Action Lawsuits

- Lawsuit filed against Cedars-Sinai Medical Center – February 2023
  - Alleged impermissible disclosures of ePHI to Google, Meta, and other third parties due to the use of website tracking technologies without either a business associate agreement with the code providers or authorizations from patients.
- Lawsuit filed against Mount Nittany Health – April 2023:
  - Alleged use of tracking code on its website and the impermissible disclosure of sensitive patient data to third parties such as Google and Facebook.

In Closing

- Evaluate – are tracking technologies worth the risk for your organization?
  - If Yes – Return to Slide 6
- Keep in mind that, even through the OCR may be slow in auditing against the guidance provided in the bulletin, consumers (in your case, participants) are strong defenders of their privacy, and class action lawsuits may be quicker to occur than formal audits.

Questions?

Agenda – DOL Cybersecurity Review

1. DOL Publications on Cybersecurity “Best Practices”
2. Findings and Review of Segal’s “DOL Best Practices” Assessments
3. Findings and Review of Segal’s Third Party (Vendor) Risk Assessments

DOL Publications on Cybersecurity Program Best Practices

April of 2021

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employ
use by reco
and data, a
should hire.

1. Ha
2. Co
3. Ha
4. Cle
5. Ha
6. Ens
   pro
   ass
7. Co

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

As sponsors of 401(k) and other types of pension plans, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of

1.

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

ONLINE SECURITY TIPS

You can reduce the risk of fraud and loss to your retirement account by following these basic rules:

- **REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT**
  - Maintaining online access to your retirement account allows you to protect and manage your investment.
  - Regularly checking your retirement account reduces the risk of fraudulent account access.
  - Failing to register for an online account may enable cybercriminals to assume your online identify.

Some Key Context for the Publications

ERISA Duty of Prudence. To paraphrase – my understanding as an operations and IT executive (not a legal interpretation):

- ERISA's duty of prudence requires fiduciaries to act with care, skill, prudence and diligence under circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.
- This has meant (previously) that ERISA fiduciaries have some responsibility to try to limit risks associated with a plan's cybersecurity exposure.
- Then the DOL (Employee Benefits Security Administration (EBSA)) issued its guidance in April of 2021
- It is now clearer what the DOL expects a prudent fiduciary to do.14

Also…the ERISA Advisory Council of 2016 published a report directed to the Secretary of Labor titled "Cybersecurity Considerations for Benefit Plans". This report raised questions about data protection for Plan fiduciaries – as it related to third parties that provided services to the Plan.

Also…in 2021 the GAO published a report that looked at that topic in more detail – specifically for defined contribution (DC) Plans and the third parties they share(d) data with to provide services to the Plan (and participants). It noted associated cybersecurity risks and recommended the DOL make it clear (formally) whether it is an ERISA fiduciary responsibility to mitigate cybersecurity risks (specifically for DC plans). The GAO recommended minimum expectations be set.

The DOL has publicly stated the cybersecurity is a priority, especially considering the size of assets that Plans hold.

There has also been private litigation related to fiduciaries' responsibility to protect Plan data and information.

Segal's Goals for its DOL Cybersecurity Program Assessments

1 Assess an organization's internal cybersecurity practices against DOL Guidelines, aka the "Cybersecurity Best Practices."

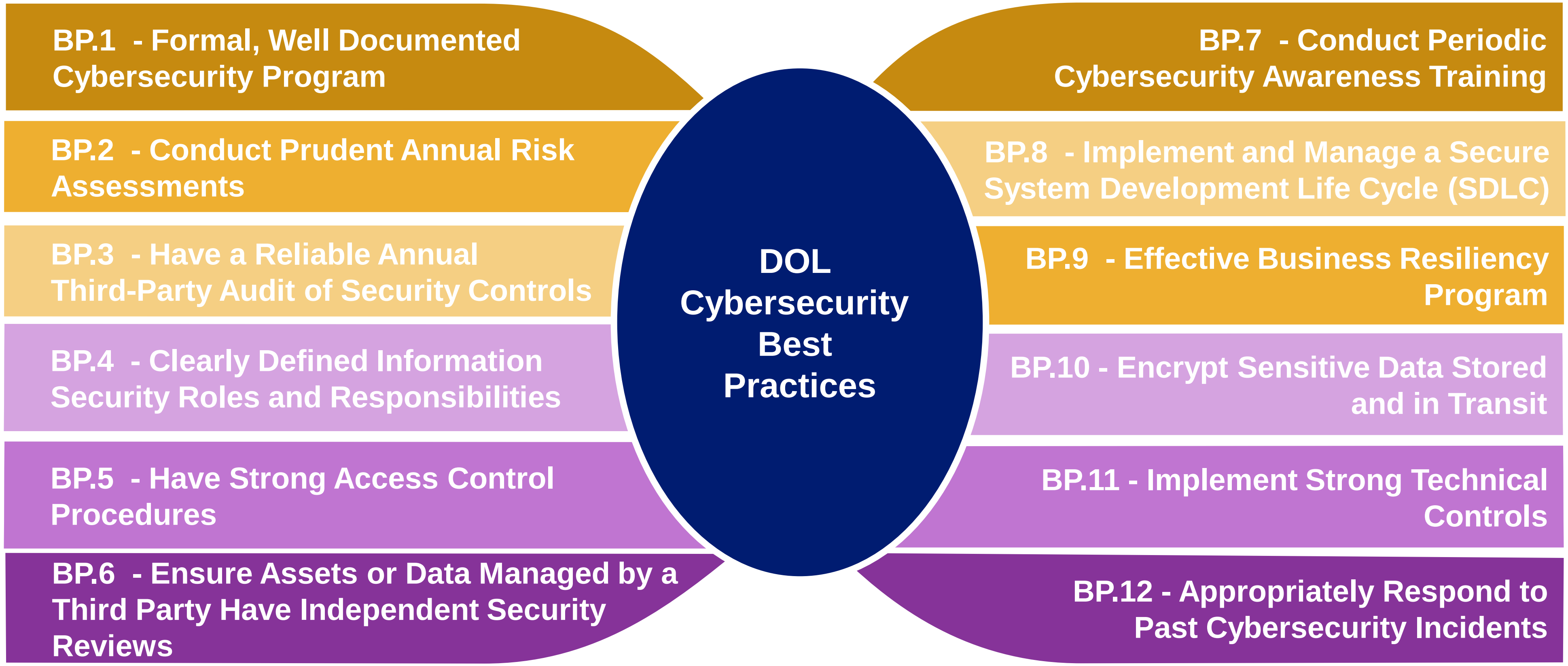
2 Assess vendors to ensure the organization has established a process for hiring service providers with strong cybersecurity practices.

3 Provide you with online security tips for participants, for your review, consideration, and ultimately to distribute as appropriate.

Today we are only discussing 1 and 2.

DOL Cybersecurity “Best Practices” 12 Categories, 75+ Elements

1



DOL Cybersecurity Best Practices

BP.1 - Formal, Well Documented Cybersecurity Program

BP.2 - Conduct Prudent Annual Risk Assessments

BP.3 - Have a Reliable Annual Third-Party Audit of Security Controls

BP.4 - Clearly Defined Information Security Roles and Responsibilities

BP.5 - Have Strong Access Control Procedures

BP.6 - Ensure Assets or Data Managed by a Third Party Have Independent Security Reviews

BP.7 - Conduct Periodic Cybersecurity Awareness Training

BP.8 - Implement and Manage a Secure System Development Life Cycle (SDLC)

BP.9 - Effective Business Resiliency Program

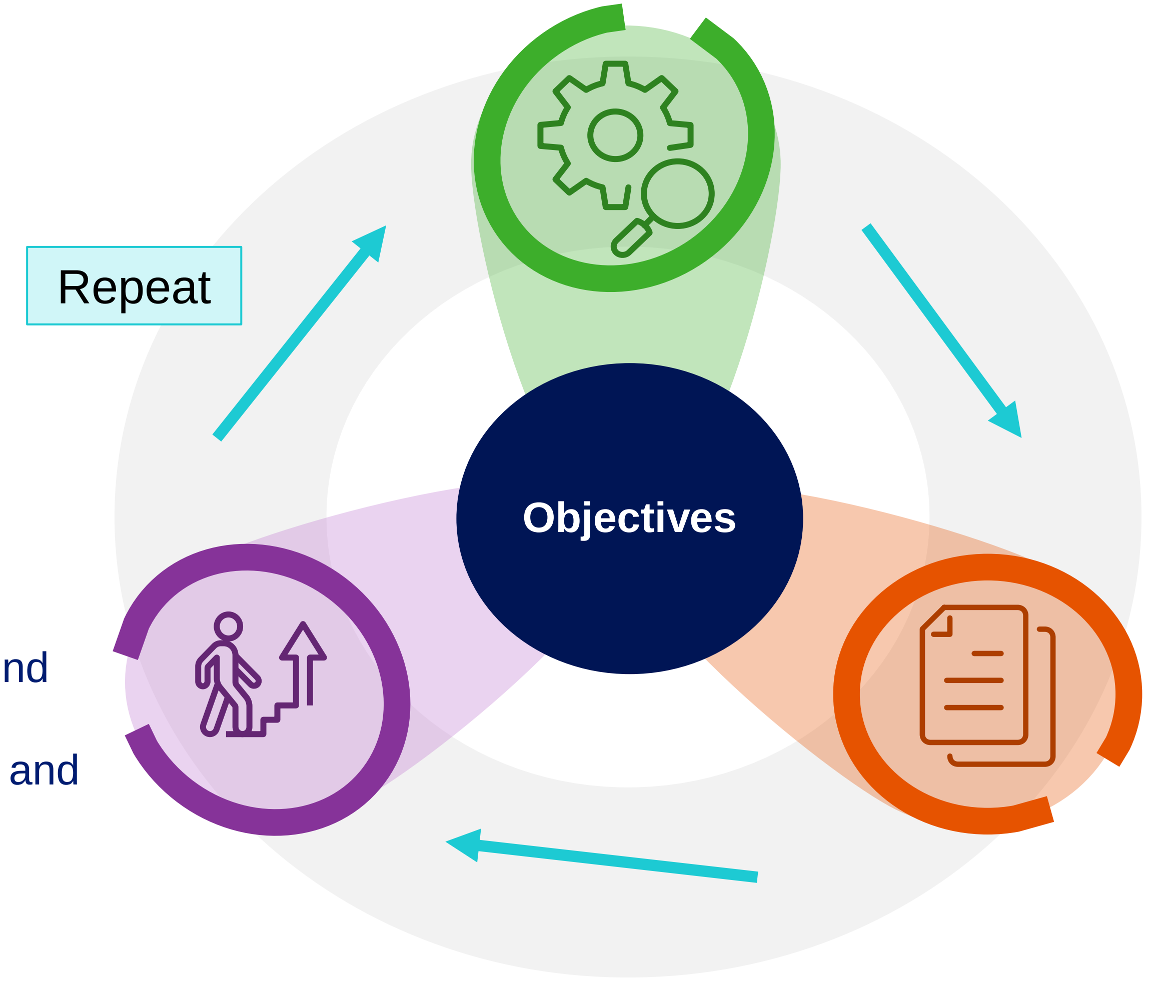
BP.10 - Encrypt Sensitive Data Stored and in Transit

BP.11 - Implement Strong Technical Controls

BP.12 - Appropriately Respond to Past Cybersecurity Incidents

https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

Segal's "Best Practices" Evaluation Objectives



A. Assess current cybersecurity activities against the Department of Labor's (DOL) "Best Practices."

B. Provide a detailed report illustrating specific actions organizations can take to enhance their cybersecurity protection.

C. Recommend improvement opportunities and next steps.

Segal’s Approach to a “Best Practices” Cybersecurity Risk Assessment

- Prepare and submit a data request that includes information related to the current cybersecurity technology, staffing, and documentation in place at the Plans (60+ questions)
- Receive and review the responses to the data request – answers to questions; review assets provided
- Schedule and conduct –as needed- interviews with the Plans to clarify data and information about:
  - Cybersecurity program roles, responsibilities, policies and processes
  - Current IT infrastructure and configurations
  - Current network vulnerability
  - Understanding the encryption methods, technologies and safeguards
  - Data classification policies, procedures and documentation
  - Business partner agreements
  - Use of mobile or portable storage, cloud, social media, etc.
  - Incident response and disaster recovery plans
  - Security training classes for all personnel
  - Policies and procedures for overall risk management

Analyzing Population Level Results – Segal "Best Practices" Risk Assessments

12 / 75+

12 Categories / 75+ Individual Elements

Segal evaluated organizations against the DOL's "Best Practices" guidance which has 12 categories and 75+ individual elements.

Segal performs a "gap analysis" comparing the "as is" state to the "should be" state.

This was an attestation by the organization. Segal took what was provided. *Not an audit.*

78

78 Client Engagements

Segal has been asked by 78 organizations to perform these risk assessments.

These may be in addition to Segal performing HIPAA-HITECH risk assessments and/or NIST (CSF) risk assessments.

39

39 Complete Engagements

Segal has completed 39 of the DOL "Best Practices" risk assessments.

Others have deferred starts by clients (for a variety of reasons).

"Best Practices" Assessments Population Level Findings

	Mean	minimum	Median	maximum
Overall Score out of 100 →	**24**	**0**	**19**	**70**
Formal, Well Documented Cybersecurity Program	2	0	1.8	4
Conduct Prudent Annual Risk Assessments	2	0	1.5	5
Have a Reliable Annual Third Party Audit of Security Controls	2	0	0	10
Clearly Defined Information Security Roles and Responsibilities	2	0	1.5	5
Have Strong Access Control Procedures	3	0	2	13
Ensure Assets or Data Managed by a Third Party Have Independent Security Reviews	2	0	0	5
Conduct Periodic Cybersecurity Awareness Training	2	0	1.5	5
Implement and Manage a Secure System Development Life Cycle (SDLC)	1	0	.5	5
Effective Business Resiliency Program	1	0	.8	5
Encrypt Sensitive Data Stored and in Transit	3	0	.4	11
Implement Strong Technical Controls	5	0	4.5	14
Appropriately Respond to Past Cybersecurity Incidents	1	0	.4	2

Goal → 60

“Best Practices” Assessments Population Level Observations

We are not saying this indicates these organizations are at a very high risk of suffering a breach, in general.

That is a function of many variables, including the total population of organizations with confidential, sensitive, nonpublic data and information in the United States, their public defenses, the ability of criminals to automate probing those defenses and the ability of criminals to penetrate and exploit those defenses, among many other variables.

We are saying this indicates these organizations are at a very high risk of suffering a breach, if they are noticed (and then targeted).

If they are targeted, the likelihood of those we have assessed to actually protect and defend the confidential, sensitive, nonpublic data and information within their management is quite low, based on our findings.

It is highly likely that sensitive data can be exfiltrated. The organization may likely suffer an actual “breach”.

Service Provider Risk Assessment High Level Population Level Findings

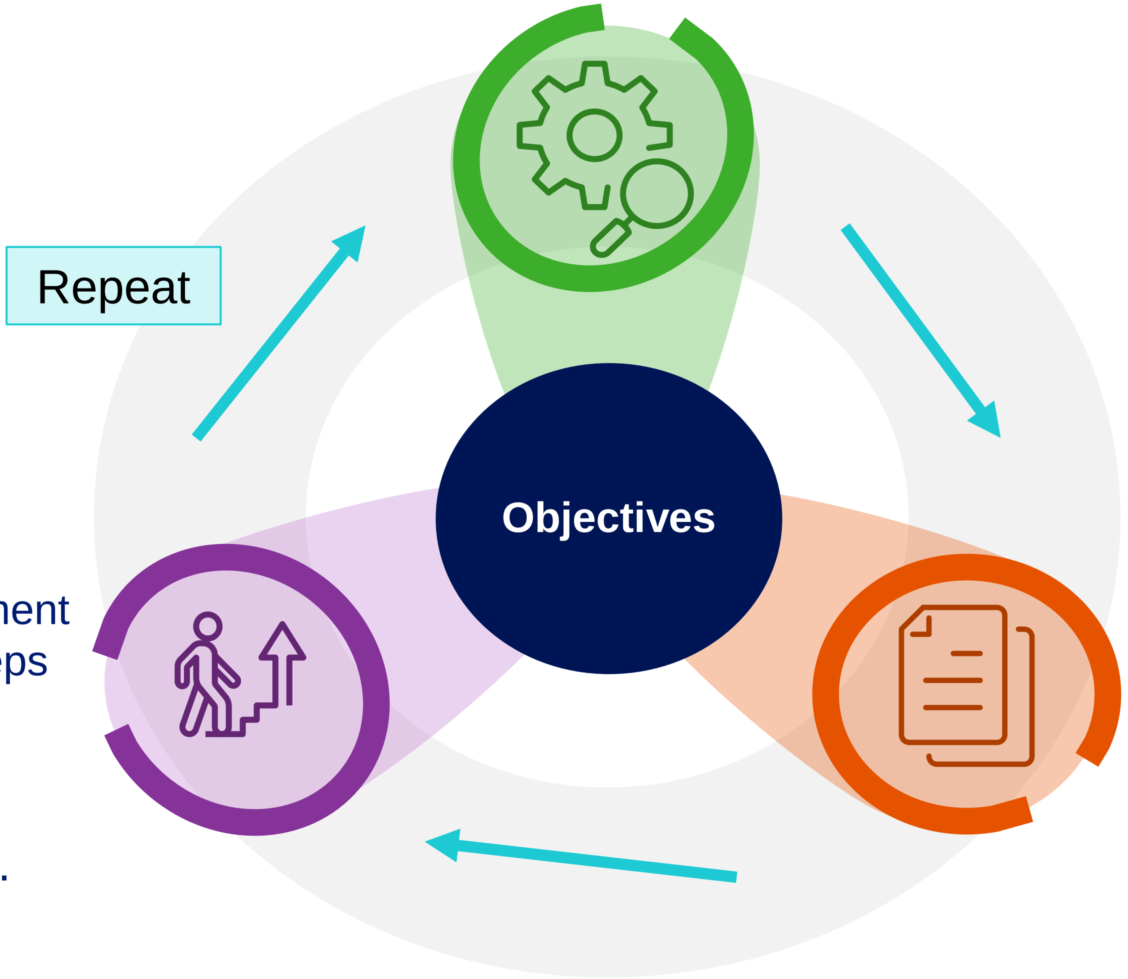
- Segal also assessed service providers for our clients.
- This was an attestation process also, again, not an audit.
- Service providers were asked questions and those answers were scored.
- Their overall scores were then grouped by ranges, by Segal's proprietary scoring rubric into **an opinion of their cybersecurity maturity**.

← **More Risk** **Less Risk** →

0 – 55%	56 – 72%	73 – 85%	86 – 100%
Insufficient	Basic	Intermediate	Advanced

Segal's Evaluation Objectives to Assist With Hiring a Service Provider With Good Cybersecurity Practices

2



A. Assess vendors cybersecurity activities against the Department of Labor's (DOL) "Best Practices", HIPAA-HITECH, ERISA, and general cybersecurity "best practices".

B. Provide various reports illustrating vendors' "general" cybersecurity stance, via different dimensions.

C. Recommend improvement opportunities and next steps for fiduciaries – highlight vendors of particular risk. Have conversations surrounding improvement.

Segal's Approach for Helping Funds Hire a Service Provider With Good Cybersecurity Practices

- Segal worked with Plans' stakeholders to implement processes and procedures allowing Segal to survey, assess (and then monitor as requested) third-party vendors, trading partners and service providers' cybersecurity programs.

- As part of this process, Segal:
  - Held meetings with the Plans to discuss the establishment of an information security governance committee (ISGC) or alternative governing and reporting structure – usually was decided an informal ad hoc group of Counsels, plan professionals, etc.
  - In partnership with that group, Segal confirmed or identified the third-party vendors to survey.
  - In partnership with that group, Segal established how it would survey those vendors (agree upon the actual survey of questions); or Segal simply took what was already distributed by the Plan.
  - Managed the survey process and scoring and reporting upon the individual vendor surveys, if Segal managed the survey process. Alternatively, Segal, would analyze and score the results if the Plan itself managed that survey process (rare, but has and is happening).

Segal’s Approach for Helping Funds Hire a Service Provider With Good Cybersecurity Practices

Survey Agreed Upon Vendors

- Inquire about information security standards, practices and policies, and audit results, and compare that information to industry standards adopted by other service providers
- Ask how the service provider validates its cybersecurity practices and what levels of security standards are in place
- Evaluate the service provider’s “track record” in the industry
- Ask about past security breaches and how the service provider responded to them
- Find out if the service provider has any insurance policies that cover losses from cybersecurity and identity theft breaches

Contracting

- Contracting was also referenced in the Guidelines; however, Segal defers to Legal Counsel. Segal was occasionally (rarely) asked to review individual elements being added to an existing Agreement.

The Population – Service Provider Risk Assessments

150+

150+ Possible Questions

Segal evaluated organizations against the DOL's "Best Practices" guidance which has 12 categories and 75+ individual elements.

Segal performs a "gap analysis" comparing the "as is" state to the "should be" state.

This was an attestation by the organization. Segal took what was provided. **Not an audit**.

108

108 Client Engagements

Segal has been asked by 108 organizations to perform these risk assessments.

These may be in addition to Segal performing HIPAA-HITECH risk assessments and/or NIST (CSF) risk assessments.

52

52 "Mostly" Complete Engagements

Segal has completed 52 of the DOL "Best Practices" risk assessments.

Others have deferred starts by clients (for a variety of reasons).

Service Provider Risk Assessment
High Level Population Level Findings

- Survey “A” – No Health Questions (service providers had no ePHI).
- 693 individual vendor questionnaires across 52 (clients)
  - Minimum count of questions – 35
  - Maximum count of questions – 109
  - Median count of questions – 56

- Based on a 60% response rate
- Minimum count of vendors – 1
- Maximum count of vendors – 87
- Median count of vendors - 11

  - 1200 points possible (regardless of question count)
    - Minimum score – 50
    - Maximum score – 1200
    - Median score – 1118
    - Median percent – 93%

Service Provider Risk Assessment
High Level Population Level Findings

- Survey “B” – Health Questions (service providers had ePHI).
- 400 individual vendor questionnaires across 52 (clients)
  - Minimum count of questions – 44
  - Maximum count of questions – 136
  - Median count of questions – 75

- Based on a 60% response rate
- Minimum count of vendors – 2
- Maximum count of vendors – 61
- Median count of vendors - 9

  - 1500 points possible (regardless of question count)
    - Minimum score – 996
    - Maximum score – 1500
    - Median score – 1305
    - Median percent – 87%

Service Provider Risk Assessment
High Level Population Level Findings

- Custom Surveys (other than ‘a’ or ‘b’ above) – more than just a few custom questions added (which are common on survey types ‘a’ and ‘b’, these are completely custom surveys).

- 126 individual vendor questionnaires across 7 (clients)
  - Minimum count of questions – 43
  - Maximum count of questions – 138
  - Median count of questions – 66

  - 1500 points possible (regardless of question count)
    - Minimum score – 300
    - Maximum score – 1500
    - Median score – 1037
    - Median percent – 65%

Service Provider Risk Assessment High Level Population Level Findings

- Computer Services and Security Providers (MSPs, MSSPs, etc.)
  - 58 unique service providers
  - Median score – 1046
  - Median percent – 65%
- Financial Service Providers – banks, and others
  - 27 unique service providers
  - Median score – 1165 median
  - Median percent – 73%

Service Provider Risk Assessment
High Level Population Level Findings

- Insurance Companies (health and all types)
  - 116 unique service providers
  - Median score – 1313
  - Median percent – 82%
- Investment Consultants
  - 32 unique service providers
  - Median score – 1140
  - Median percent – 71%

Service Provider Risk Assessment
High Level Population Level Findings

- Investment Managers
  - 160 unique service providers
  - Median score – 1138
  - Median percent – 71%
- Professional Service Providers
  - 199 unique service providers
  - Median score – 1130
  - Median percent – 71%
- Vendors
  - 130 unique service providers
  - Median score – 1130
  - Median percent – 71%

“Service Provider” Assessments Population Level Observations

This data does not necessarily indicate these clients are at a low risk of suffering a breach, in general, due to their vendors.

Why not?

As one may note, overall the population is scoring at least “basic” (by vendor category) in their median percents. And the median percents for those who do and do not manage PII versus ePHI is also quite high.

From different perspectives, the service provider population seems to be doing “fine” to “well”.

However…third party risk is cumulative. The more service providers you have the higher your population risk.

To illustrate cumulative risk from service providers, let’s look at the hypothetical scenario below:

One (1) service provider is quite mature in their cybersecurity practices, and so they score an ‘advanced’ rating. Good.

For the sake of illustration let’s say they have a .05 chance of a breach. (99.95% chance they won’t have a breach.)

Let’s say you have 10 vendors that fit the same profile.

Your overall service provider population chance of a breach is:

10 x .005 = .05 or a 5% chance of a breach within your population – all things being equal – in this illustration!

That seems high, actually!

Questions?

Thank You

For more info, please contact us

mstoyanovich@segalco.com
248-910-2637

kzinnen@segalco.com
415.470.0159

Multiemployer IT Summit

What's NExT?

The 3 Ts: Technology, Turnaround & Transformation (including AI)

Joel Manfredo, Chief Information, Innovation & Digital Officer, Motion Picture Industry Pension & Health Plans

October 10-11, 2023 / San Diego

Proudly sponsored by

Segal

Agenda:

1. Takeaways
2. Company Background
3. Transformation, Turnaround, Technology
4. Digital Transformation / “Hyperautomation”
5. Sustained Enablement
6. Innovation, ML/AI, LLM at MPI
7. Co-Pilots
8. Q&A

Takeaways

PSCBD (I’ll explain later)

Organizational Maturity: Project → Program → Product

Digital Transformation: Multifaceted, organization defined, near infinite possibilities

Machine Learning, Artificial Intelligence, Generative Pre-Trained Transformer: Don’t go it alone

MPI: Company Background

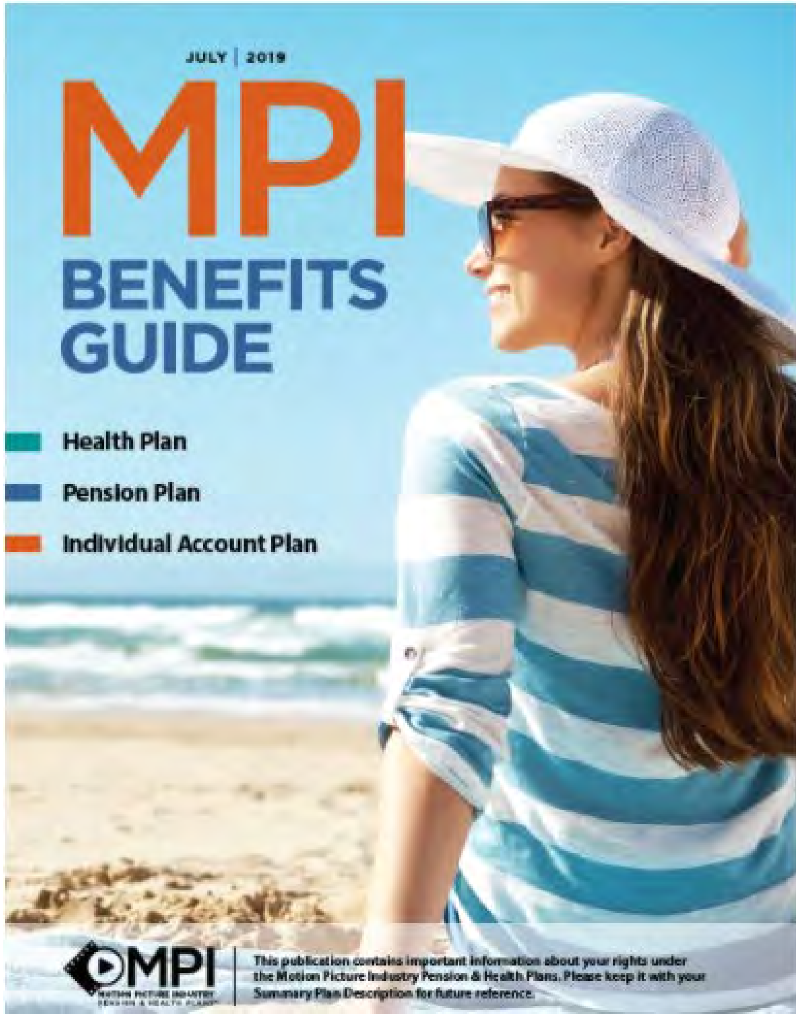
History and Business

- Taft-Hartley Multi-Employer Plan, 1952
- Administrator of Health & Pension Benefits

Statistics

2022	Active	Retiree	Total
Average Eligibles	62,115	16,798	78,913
Covered Lives	120,001	26,002	146,003

- As of 12/31/22
- 40 Unions
- 1,200 – 1,400 Employers
- Employees – 327 total; 43 in IT
- Sources of “Revenue”: contributions, residuals, audits, investment returns ~ $3.0 billion
- $11.7 Billion in invested assets



JULY | 2019

MPI

BENEFITS GUIDE

🟩 Health Plan

🟦 Pension Plan

🟧 Individual Account Plan

MPI MOTION PICTURE INDUSTRY PENSION & HEALTH PLANS

This publication contains important information about your rights under the Motion Picture Industry Pension & Health Plans. Please keep it with your Summary Plan Description for future reference.

State of Information Technology

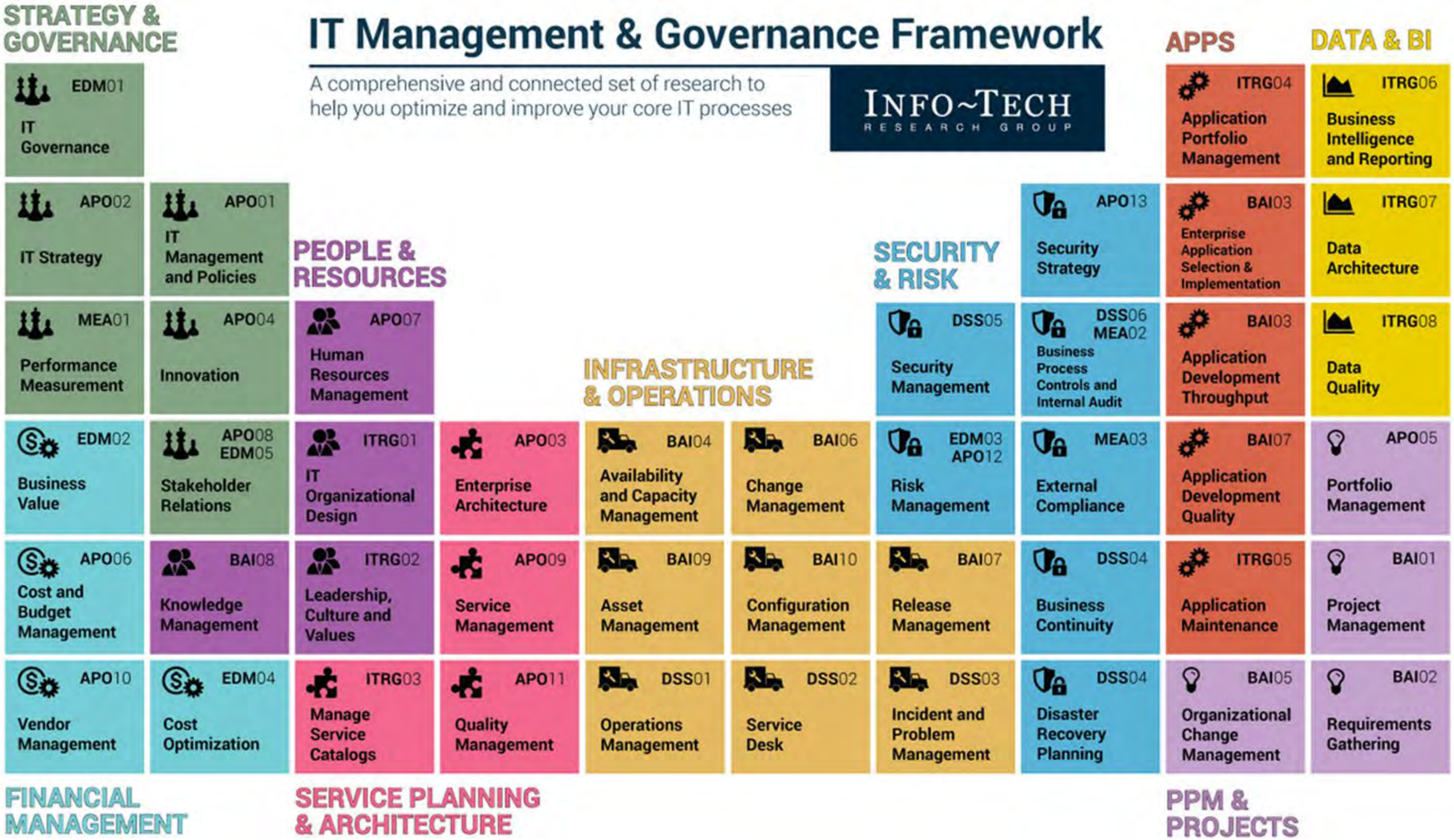
Infrastructure

- Data Center
- Compute (Network, SAN, Backup, Servers)
- Security

Applications

- Claims & Pension
- Supporting (Contracts & Contributions, Eligibility & Premiums, Audit & Collections and Residuals & Deposits) – VB 6
- Outages

State of Information Technology



STRATEGY & GOVERNANCE

IT Management & Governance Framework

A comprehensive and connected set of research to help you optimize and improve your core IT processes

INFO~TECH RESEARCH GROUP

APPS

DATA & BI

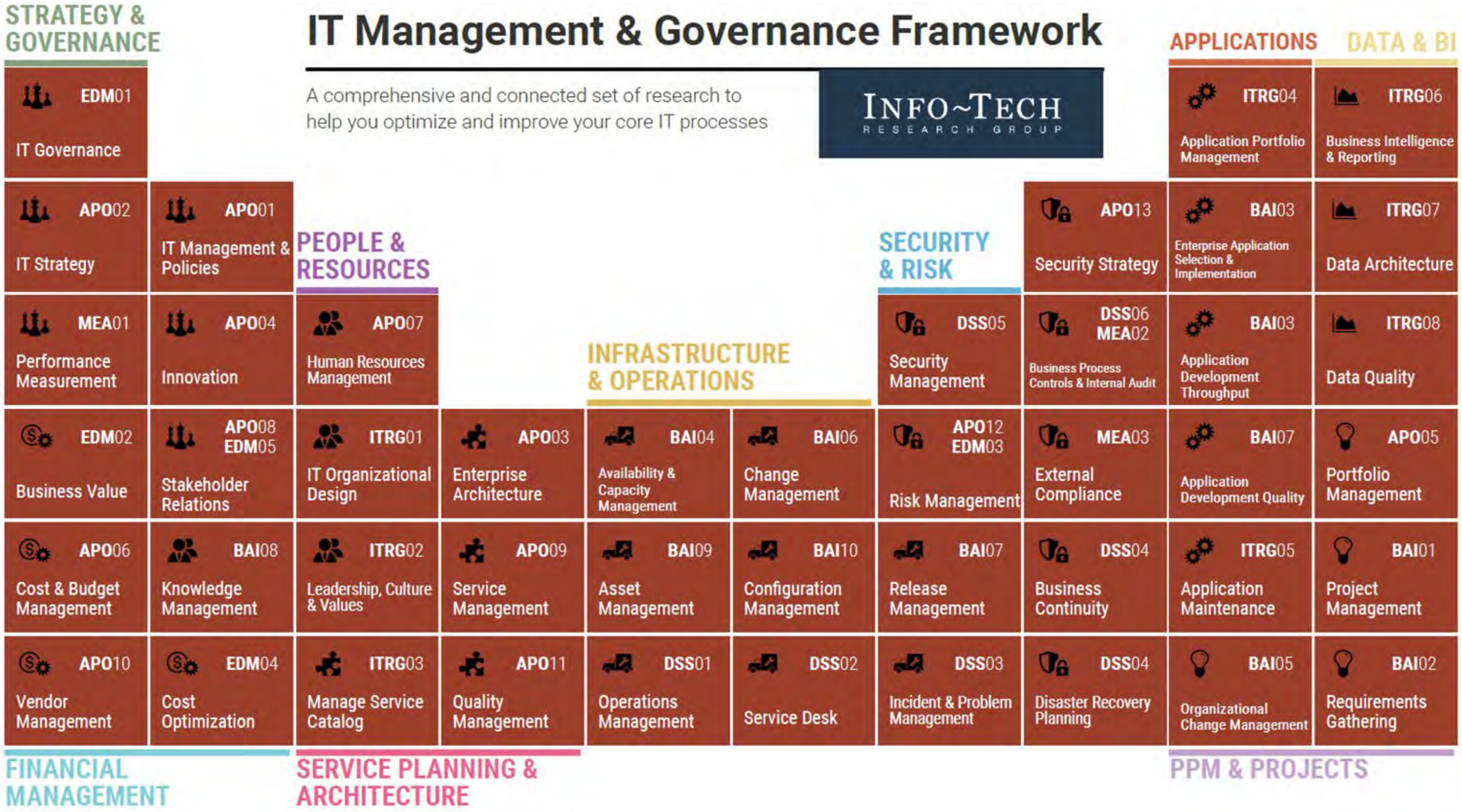
EDM01 IT Governance								ITRG04 Application Portfolio Management	ITRG06 Business Intelligence and Reporting
APO02 IT Strategy	APO01 IT Management and Policies	PEOPLE & RESOURCES				SECURITY & RISK	APO13 Security Strategy	BAI03 Enterprise Application Selection & Implementation	ITRG07 Data Architecture
MEA01 Performance Measurement	APO04 Innovation	APO07 Human Resources Management		INFRASTRUCTURE & OPERATIONS		DSS05 Security Management	DSS06 MEA02 Business Process Controls and Internal Audit	BAI03 Application Development Throughput	ITRG08 Data Quality
EDM02 Business Value	APO08 EDM05 Stakeholder Relations	ITRG01 IT Organizational Design	APO03 Enterprise Architecture	BAI04 Availability and Capacity Management	BAI06 Change Management	EDM03 APO12 Risk Management	MEA03 External Compliance	BAI07 Application Development Quality	APO05 Portfolio Management
APO06 Cost and Budget Management	BAI08 Knowledge Management	ITRG02 Leadership, Culture and Values	APO09 Service Management	BAI09 Asset Management	BAI10 Configuration Management	BAI07 Release Management	DSS04 Business Continuity	ITRG05 Application Maintenance	BAI01 Project Management
APO10 Vendor Management	EDM04 Cost Optimization	ITRG03 Manage Service Catalogs	APO11 Quality Management	DSS01 Operations Management	DSS02 Service Desk	DSS03 Incident and Problem Management	DSS04 Disaster Recovery Planning	BAI05 Organizational Change Management	BAI02 Requirements Gathering

FINANCIAL MANAGEMENT

SERVICE PLANNING & ARCHITECTURE

PPM & PROJECTS

State of Information Technology



IT Management & Governance Framework

A comprehensive and connected set of research to help you optimize and improve your core IT processes

INFO~TECH RESEARCH GROUP

STRATEGY & GOVERNANCE								APPLICATIONS	DATA & BI
EDM01 IT Governance								ITRG04 Application Portfolio Management	ITRG06 Business Intelligence & Reporting
APO02 IT Strategy	APO01 IT Management & Policies	PEOPLE & RESOURCES				SECURITY & RISK	APO13 Security Strategy	BAI03 Enterprise Application Selection & Implementation	ITRG07 Data Architecture
MEA01 Performance Measurement	APO04 Innovation	APO07 Human Resources Management		INFRASTRUCTURE & OPERATIONS		DSS05 Security Management	DSS06 MEA02 Business Process Controls & Internal Audit	BAI03 Application Development Throughput	ITRG08 Data Quality
EDM02 Business Value	APO08 EDM05 Stakeholder Relations	ITRG01 IT Organizational Design	APO03 Enterprise Architecture	BAI04 Availability & Capacity Management	BAI06 Change Management	APO12 EDM03 Risk Management	MEA03 External Compliance	BAI07 Application Development Quality	APO05 Portfolio Management
APO06 Cost & Budget Management	BAI08 Knowledge Management	ITRG02 Leadership, Culture & Values	APO09 Service Management	BAI09 Asset Management	BAI10 Configuration Management	BAI07 Release Management	DSS04 Business Continuity	ITRG05 Application Maintenance	BAI01 Project Management
APO10 Vendor Management	EDM04 Cost Optimization	ITRG03 Manage Service Catalog	APO11 Quality Management	DSS01 Operations Management	DSS02 Service Desk	DSS03 Incident & Problem Management	DSS04 Disaster Recovery Planning	BAI05 Organizational Change Management	BAI02 Requirements Gathering
FINANCIAL MANAGEMENT		SERVICE PLANNING & ARCHITECTURE						PPM & PROJECTS	

State of Information Technology

What do you do?

5 Minute breakout session

State of Information Technology

General Prioritization

Production: If systems do not function well, we are left unable to service our participants optimally.

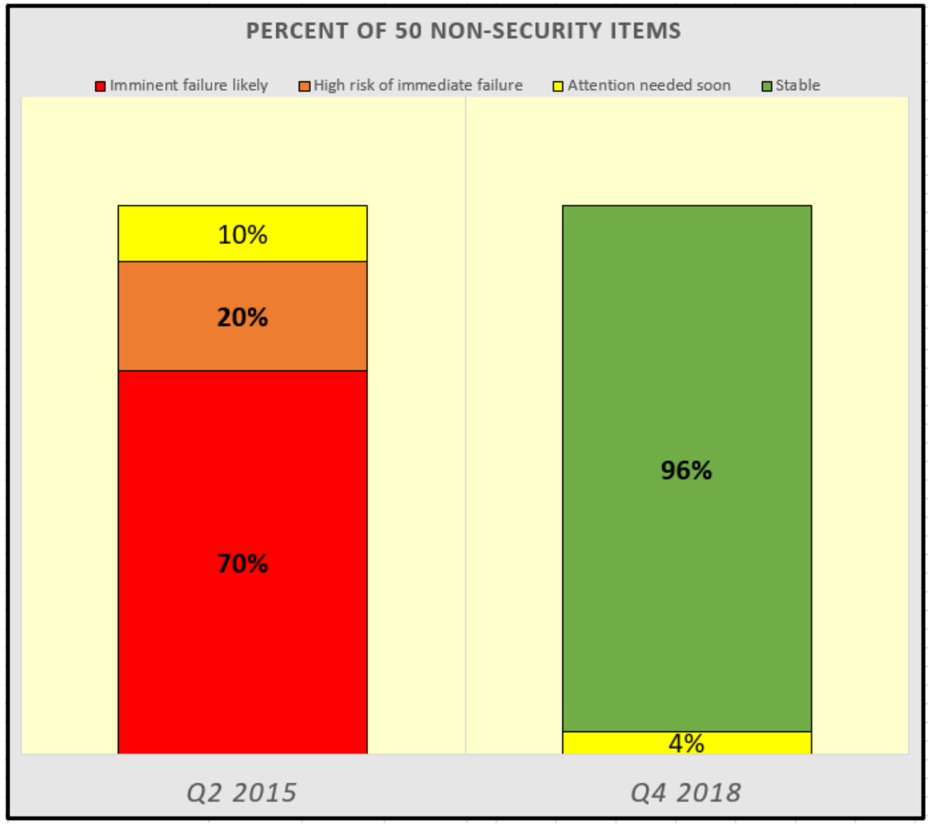
Security: Protecting our participants' data continue to be a critical priority for us.

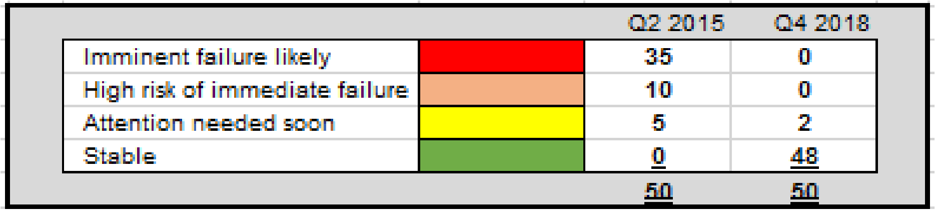
Compliance: Regulations continue to change and it is critical to maintain IT support in order to align with changes and timelines

Backups: Insufficient backups leave organization potentially susceptible to loss of participant data.

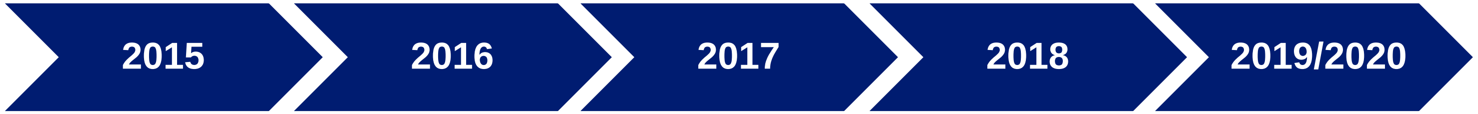
Disaster Recovery: In case of disaster, understanding how the organization will recover and how quickly lead to peace of mind.

Transformation, Turnaround, Technology





		Q2 2015	Q4 2018
Imminent failure likely	🟥	35	0
High risk of immediate failure	🟧	10	0
Attention needed soon	🟨	5	2
Stable	🟩	0	48
		50	50



2015	2016	2017	2018	2019/2020
Production Security	Production Security Backup Disaster Recovery	Production Security Backup Disaster Recovery Core System	Core System Phone System Web & Mobile App	Core System CRM Web Product ECM Strategy/RFP

Some stats...

- 216 Projects completed
- > 98% at or below cost and on scope
- > 97% on schedule
- Key issue – **get the budget!**

Transformation, Turnaround, Technology

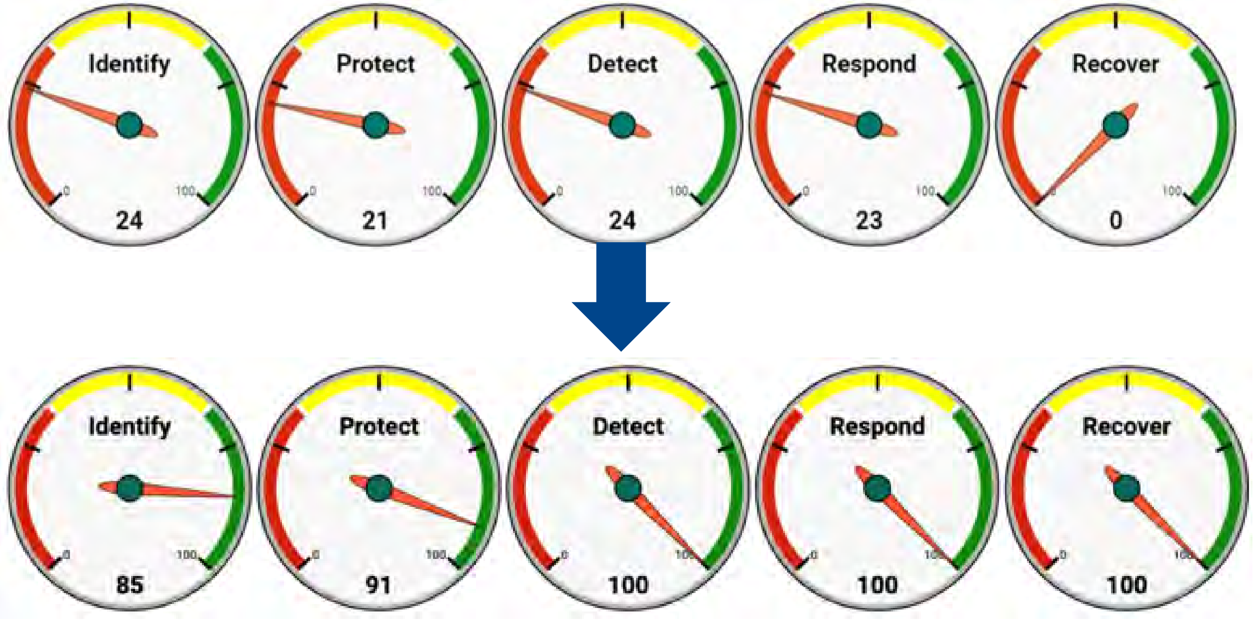
Security:

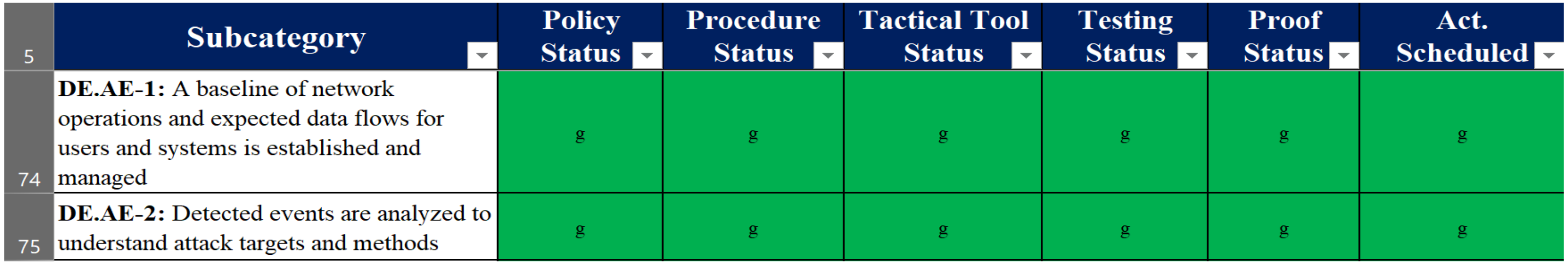
“Your data is being exfiltrated… 32 Tools, 22 months

2022 Status:

Mar 2015

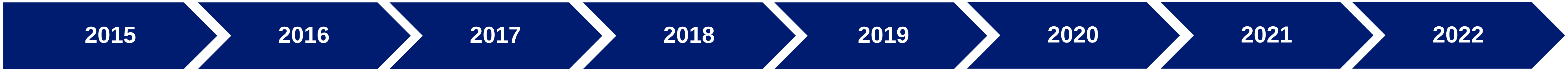
Dec 2022





5	Subcategory	Policy Status	Procedure Status	Tactical Tool Status	Testing Status	Proof Status	Act. Scheduled
74	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	g	g	g	g	g	g
75	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods	g	g	g	g	g	g

Enablement: Project → Program → Product



2015 2016 2017 2018 2019 2020 2021 2022

PROJECT ERA

PROJECT CHARACTERISTICS

Defined Objective

Defined Scope

Defined Timeframe

Defined Cost

PROGRAM ERA

PROGRAM CHARACTERISTICS

Defined Target State

Collection of Projects

ROM Timeframe

ROM Cost

PRODUCT ERA

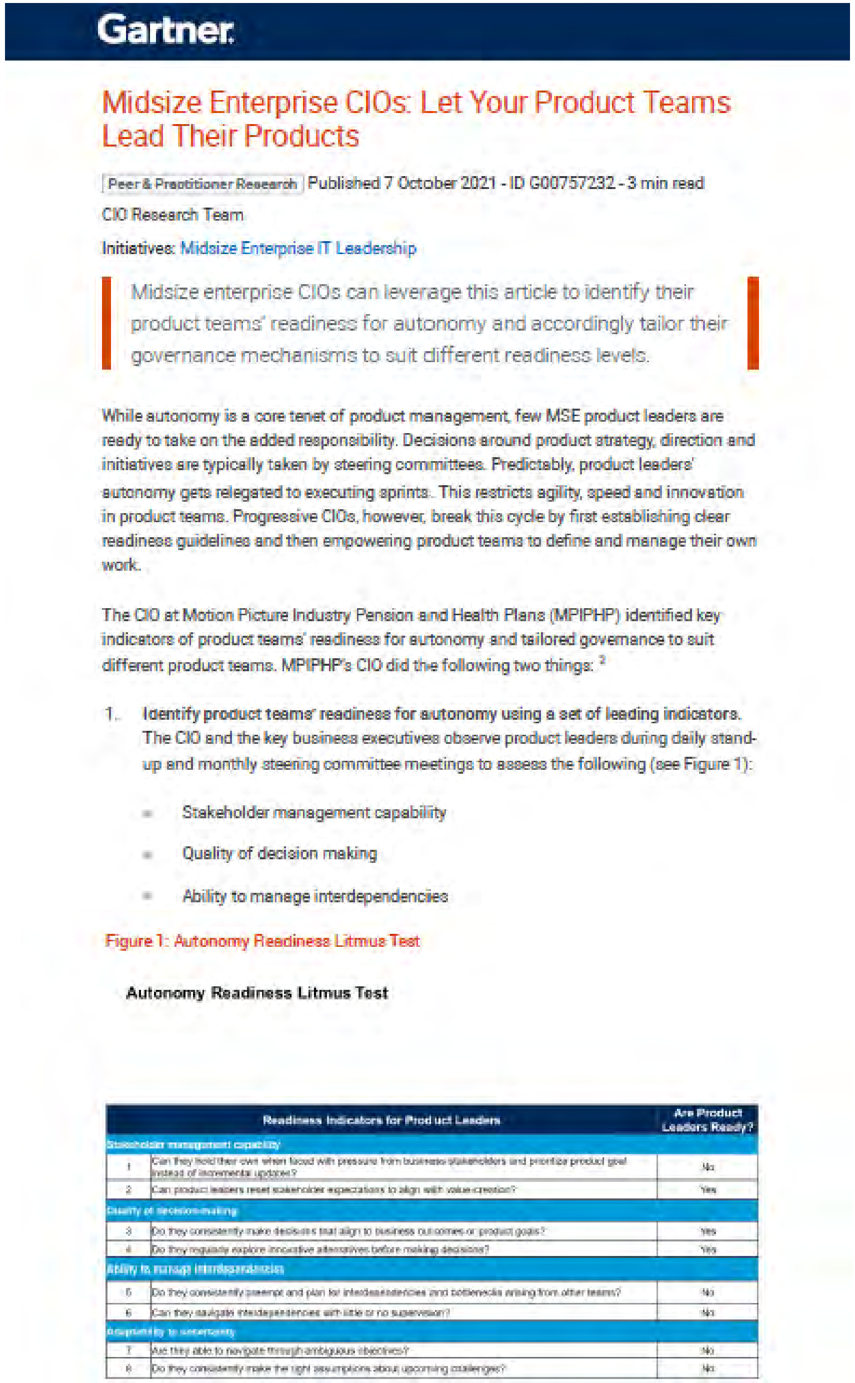
PRODUCT CHARACTERISTICS

Defined Strategic Direction

Agile Methodology

Indefinite Timeframe

Ongoing Investment Expected



Gartner

Midsize Enterprise CIOs: Let Your Product Teams Lead Their Products

Peer & Practitioner Research | Published 7 October 2021 - ID G00757232 - 3 min read

CIO Research Team

Initiatives: Midsize Enterprise IT Leadership

> Midsize enterprise CIOs can leverage this article to identify their product teams' readiness for autonomy and accordingly tailor their governance mechanisms to suit different readiness levels.

While autonomy is a core tenet of product management, few MSE product leaders are ready to take on the added responsibility. Decisions around product strategy, direction and initiatives are typically taken by steering committees. Predictably, product leaders' autonomy gets relegated to executing sprints. This restricts agility, speed and innovation in product teams. Progressive CIOs, however, break this cycle by first establishing clear readiness guidelines and then empowering product teams to define and manage their own work.

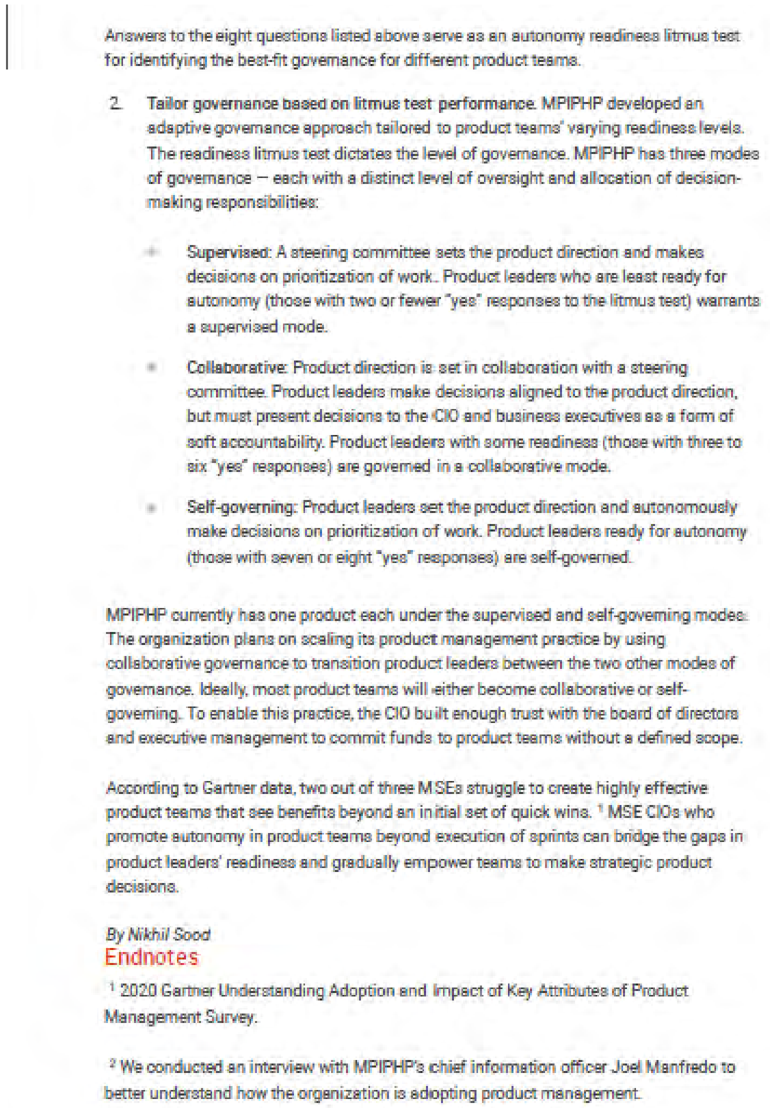
The CIO at Motion Picture Industry Pension and Health Plans (MPIPHP) identified key indicators of product teams' readiness for autonomy and tailored governance to suit different product teams. MPIPHP's CIO did the following two things: [2]

1. **Identify product teams' readiness for autonomy using a set of leading indicators.** The CIO and the key business executives observe product leaders during daily stand-up and monthly steering committee meetings to assess the following (see Figure 1):
   - Stakeholder management capability
   - Quality of decision making
   - Ability to manage interdependencies

Figure 1: Autonomy Readiness Litmus Test

Autonomy Readiness Litmus Test

	Readiness Indicators for Product Leaders	Are Product Leaders Ready?
Stakeholder management capability		
1	Can they hold their own when faced with pressure from business stakeholders and prioritize product goal instead of incremental updates?	No
2	Can product leaders reset stakeholder expectations to align with value-creation?	Yes
Quality of decision-making		
3	Do they consistently make decisions that align to business outcomes or product goals?	Yes
4	Do they regularly explore innovative alternatives before making decisions?	Yes
Ability to manage interdependencies		
5	Do they consistently preempt and plan for interdependencies and bottlenecks arising from other teams?	No
6	Can they navigate interdependencies with little or no supervision?	No
Adaptability to uncertainty		
7	Are they able to navigate through ambiguous objectives?	No
8	Do they consistently make the right assumptions about upcoming challenges?	No



Answers to the eight questions listed above serve as an autonomy readiness litmus test for identifying the best-fit governance for different product teams.

2. **Tailor governance based on litmus test performance.** MPIPHP developed an adaptive governance approach tailored to product teams' varying readiness levels. The readiness litmus test dictates the level of governance. MPIPHP has three modes of governance — each with a distinct level of oversight and allocation of decision-making responsibilities:
   - Supervised: A steering committee sets the product direction and makes decisions on prioritization of work. Product leaders who are least ready for autonomy (those with two or fewer "yes" responses to the litmus test) warrants a supervised mode.
   - Collaborative: Product direction is set in collaboration with a steering committee. Product leaders make decisions aligned to the product direction, but must present decisions to the CIO and business executives as a form of soft accountability. Product leaders with some readiness (those with three to six "yes" responses) are governed in a collaborative mode.
   - Self-governing: Product leaders set the product direction and autonomously make decisions on prioritization of work. Product leaders ready for autonomy (those with seven or eight "yes" responses) are self-governed.

MPIPHP currently has one product each under the supervised and self-governing modes. The organization plans on scaling its product management practice by using collaborative governance to transition product leaders between the two other modes of governance. Ideally, most product teams will either become collaborative or self-governing. To enable this practice, the CIO built enough trust with the board of directors and executive management to commit funds to product teams without a defined scope.

According to Gartner data, two out of three MSEs struggle to create highly effective product teams that see benefits beyond an initial set of quick wins. [1] MSE CIOs who promote autonomy in product teams beyond execution of sprints can bridge the gaps in product leaders' readiness and gradually empower teams to make strategic product decisions.

By Nikhil Sood

Endnotes

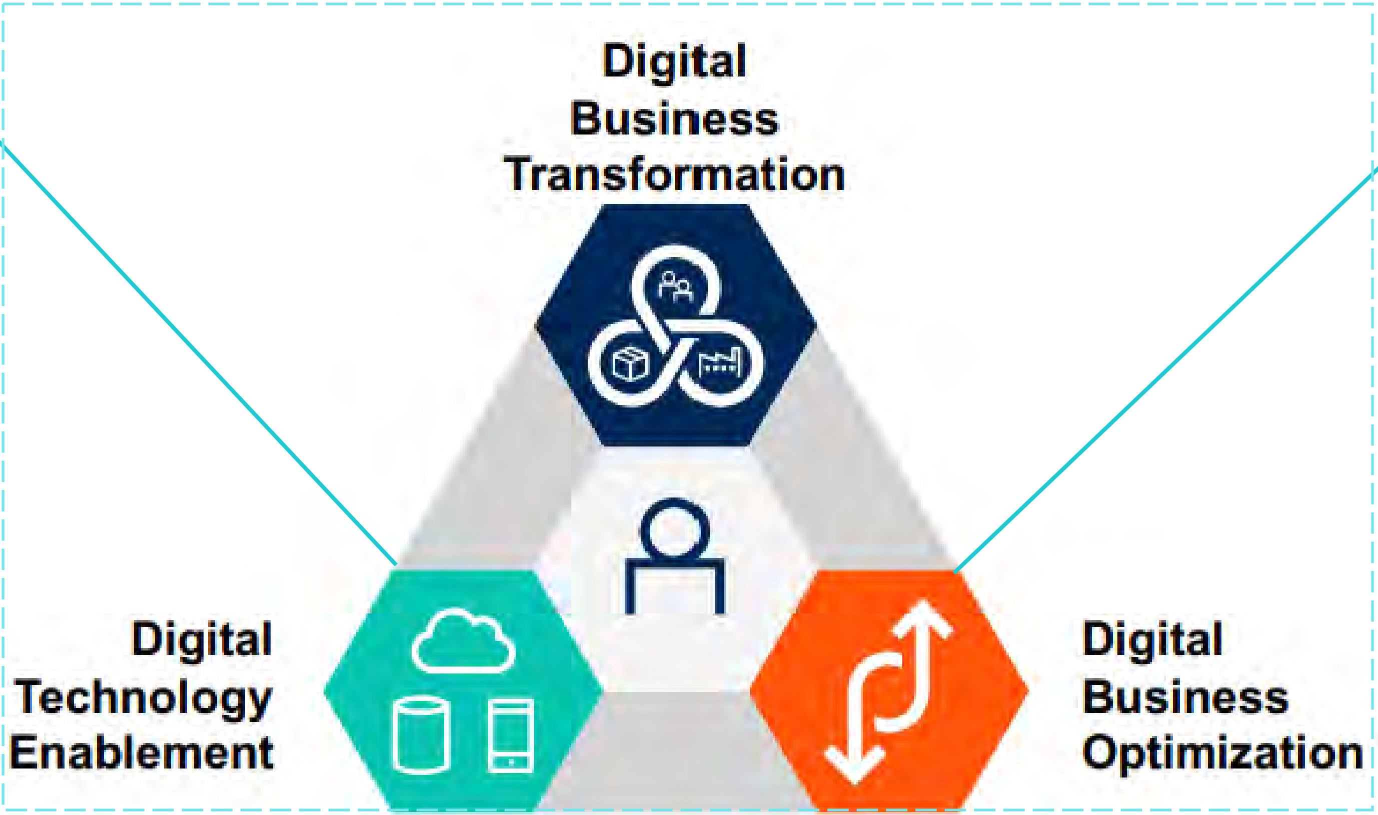
[1] 2020 Gartner Understanding Adoption and Impact of Key Attributes of Product Management Survey.

[2] We conducted an interview with MPIPHP's chief information officer Joel Manfredo to better understand how the organization is adopting product management.

Digital Transformation at MPI: What is it?

Occurs when technology is used to create new revenue streams and **digital products.**

These are the **technical foundations** of digital business. They include infrastructure and operations (including security), applications, and cloud strategies (the platforms on which digital business runs).


Digital Business Transformation
Digital Technology Enablement
Digital Business Optimization

Gartner Model

This is the use of digital technology to **improve what we already have**. It may take the form of operational efficiency, improving the customer experience, cost-saving initiatives, or revenue-enhancing ones

Digital Transformation at MPI: What is it?

Mobile Application
E-Billing Assumption
Customer Relationship Management / Call Center Telephony
Educational Video On Demand
Integration Platform as a Service ("iPaaS")
IAP Hardship Withdrawal
Chatbot (OpenAI) – "The Botfather"

Digital Business Transformation

7 %

16

Data Center Re-build
Replacement:
Network, Storage, Backup & Compute
Security program ~ 40 projects
Business Continuity / Disaster Recovery
DevOps
Resiliency Upgrades

Website Redux
Web Product (Agile Methodology)
Genesis (V3)
Data Warehouse Program
Office 365 (cloud)
QNXT, OPUS upgrades
QNXT Workflow
Video Conferencing

63 %

137

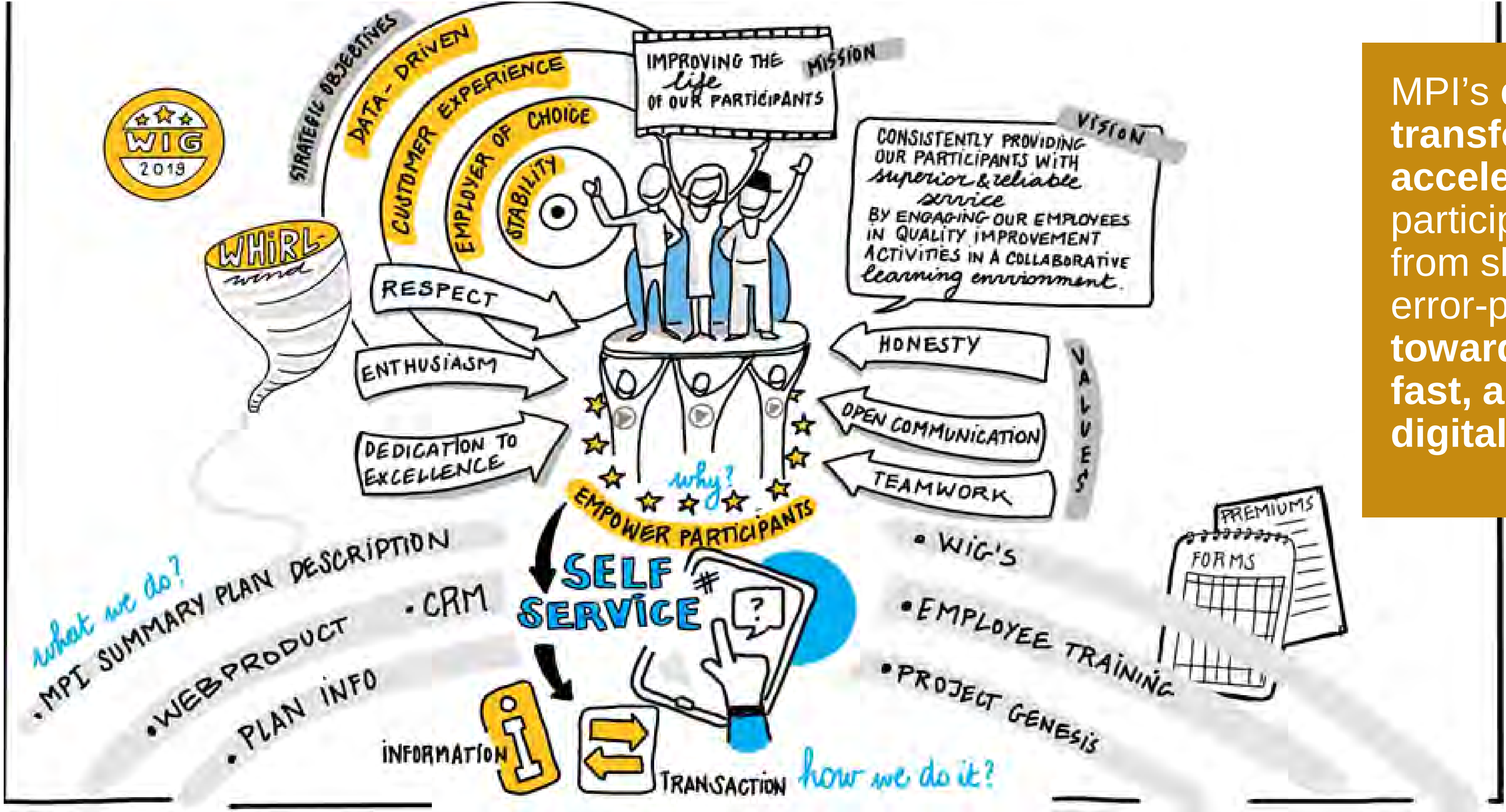
Digital Technology Enablement

Digital Business Optimization

29%

63

Digital Transformation at MPI: What is it?



MPI's **digital transformation accelerates** helping our participants by **moving** from slow, manual, error-prone processes **towards a frictionless, fast, and accurate digital** ecosystem.

Automation at MPI: Some Realized Efforts

Security Automation

- 24/7 automated monitoring and alerting of critical alerts
- Automated log correlation, reports and daily analysis
- “Kill Switch” has been automated that with 3 people concurring, we can immediately sever all connections to our network

Infrastructure & Operations

Large number of operational issues: automated alerts

Most of these efforts, particularly the bots, are single task automations.
Now, we are moving to broader process automation.

Automation at MPI: Some Realized Metrics

Website:

- 15,000 participants have opted into electronic EOBs
- 87% of Premium payments come through the website

Robotic Process Automation Bots:

- In 2021 and 2022 the Claims adjudication bot processed 19,000 claims
- Index & File Bot: since inception, in late 2020, the bot has indexed and filed 112,000 forms submitted on the website

Integration Platform as a Service (IPaaS)

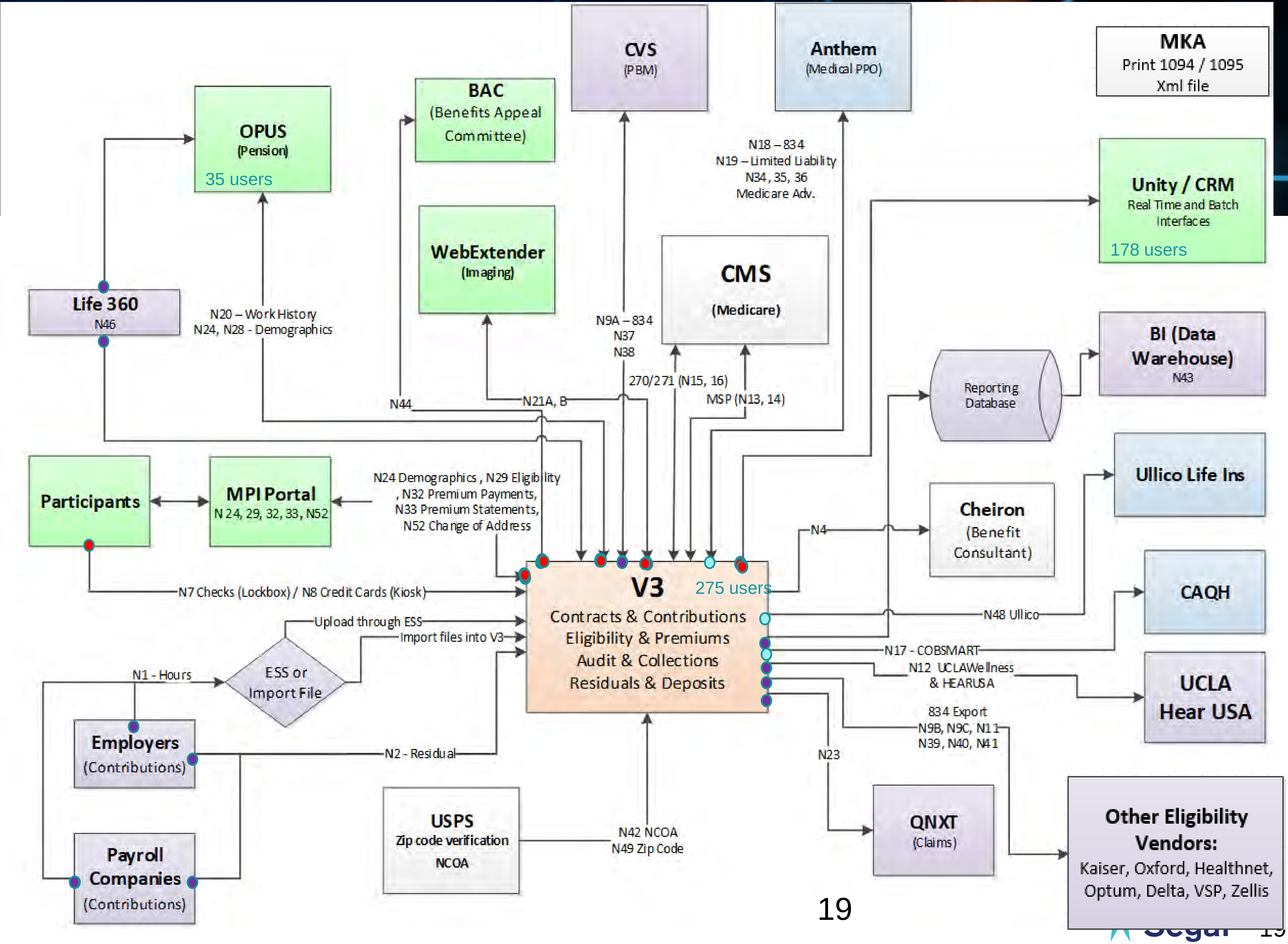
1.3 million API invocations per month

IPaaS

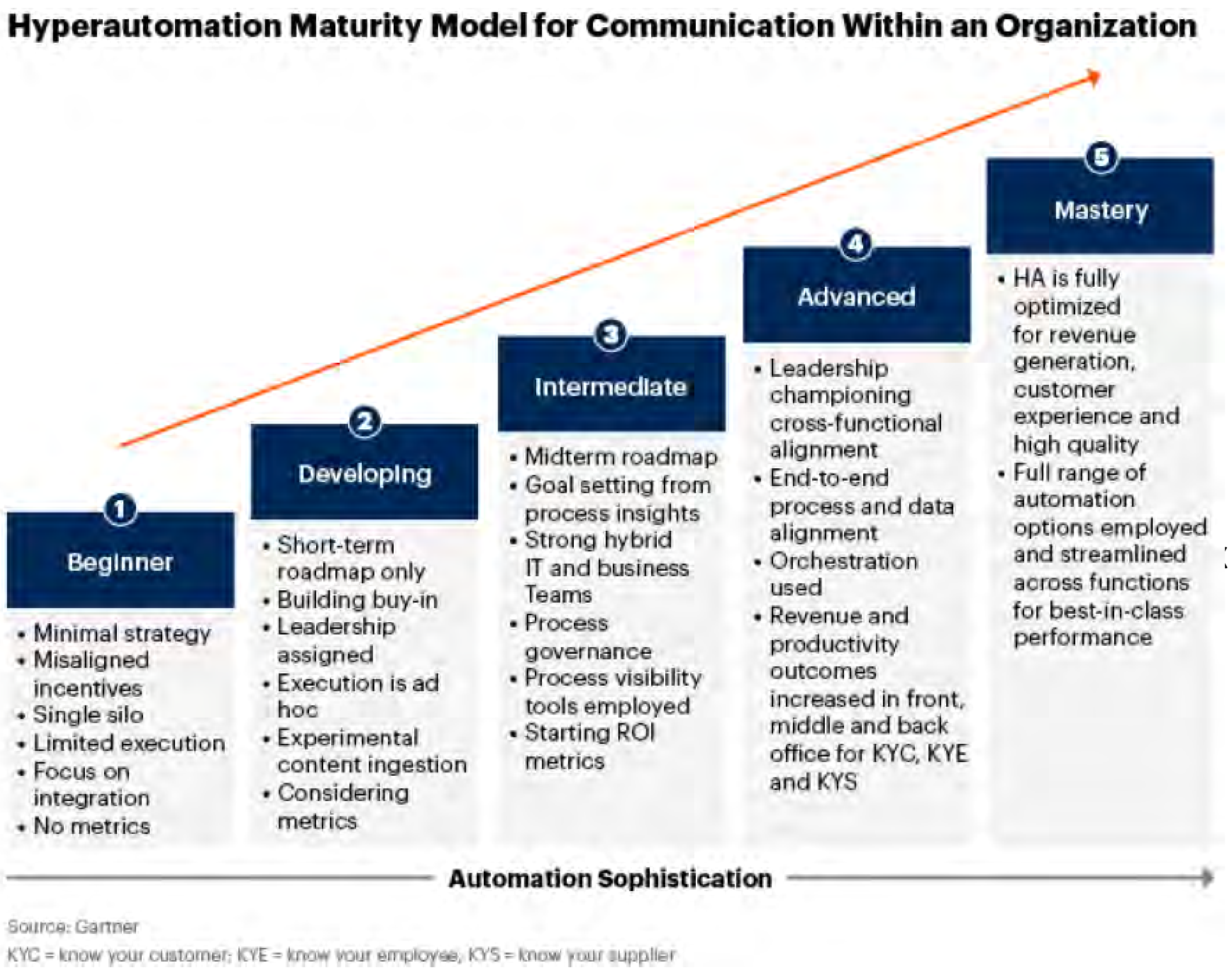
Activity Estimates:	Monthly
V3 Orchestrated Jobs	1,144
V3 File Activity	
Export	569
Import	243
Total	812
V3 API Invocations	1,265,558

65 Interfaces

Real Time	●	🟩
Daily	●	☐
Weekly	○	☐
Monthly+		☐



Automation at MPI: Some Realized Metrics



Hyperautomation Maturity Model for Communication Within an Organization

1 Beginner
- Minimal strategy
- Misaligned incentives
- Single silo
- Limited execution
- Focus on integration
- No metrics

2 Developing
- Short-term roadmap only
- Building buy-in
- Leadership assigned
- Execution is ad hoc
- Experimental content ingestion
- Considering metrics

3 Intermediate
- Midterm roadmap
- Goal setting from process insights
- Strong hybrid IT and business Teams
- Process governance
- Process visibility tools employed
- Starting ROI metrics

4 Advanced
- Leadership championing cross-functional alignment
- End-to-end process and data alignment
- Orchestration used
- Revenue and productivity outcomes increased in front, middle and back office for KYC, KYE and KYS

5 Mastery
- HA is fully optimized for revenue generation, customer experience and high quality
- Full range of automation options employed and streamlined across functions for best-in-class performance

Automation Sophistication

Source: Gartner

KYC = know your customer; KYE = know your employee, KYS = know your supplier

2023 efforts:

1) RPA project – we just signed an SOW for 18 additional bots, mostly in IT
2) Process documentation – domain experts
3) Automation expert – tool reviews, assessments and recommendations: 3 new tools required

Automation at MPI: Moving Forward

Recommended Capabilities

The identified inefficiencies can most effectively be significantly reduced by implementing:

- **Workflow:** Serves as the process backbone, enabling overall process management, orchestration, and automation
- **RPA (Robotic Process Automation):** Automates repetitive manual tasks
- **IDP (Intelligent Document Processing):** Uses AI/ML* to extract and process data from documents
- **Automation and App Development:** Provides a platform for creating applications to automate activities, e.g., a website portal for unified participant interactions and submissions
- **ECM (Enterprise Content Management):** Manages, securely shares, and automates documents and data
- **Process Mining:** Uses AI/ML on system event log data for process discovery, improvement and monitoring

Evaluated Possible Solutions

Doculabs evaluated numerous solutions against MPI's business, functional, technical, and resource requirements

Doculabs examined MPI's existing portfolio and many alternative options in relevant domains

Shortlisted Solutions

- **Workflow**: Laserfiche, Microsoft, Appian, Nintex, Pega, Workato
- **RPA**: UiPath, Kofax, Automation Anywhere, Blue Prism
- **IDP**: Laserfiche, Kofax, UiPath, Microsoft, AWS
- **Automation and App Development**: Microsoft Power Platform, Informatica IICS, Appian, AWS
- **ECM**: Laserfiche, Microsoft
- **Process Mining**: ABBYY, Celonis, Microsoft (Power Automate), UiPath

Selected Solutions

Doculabs strongly recommends the following primary solutions:

Workflow Platform: Laserfiche

RPA Suite: UiPath

IDP Suite: Microsoft Azure Cognitive Services ***(to be acquired)***

Automation and App Development Platform: Microsoft Power Platform (and continue with IICS)

ECM: Laserfiche

Process Mining: Celonis ***(to be acquired)***

Evaluate native capabilities of OPUS, V3, and QNXT for system-specific task management and automation

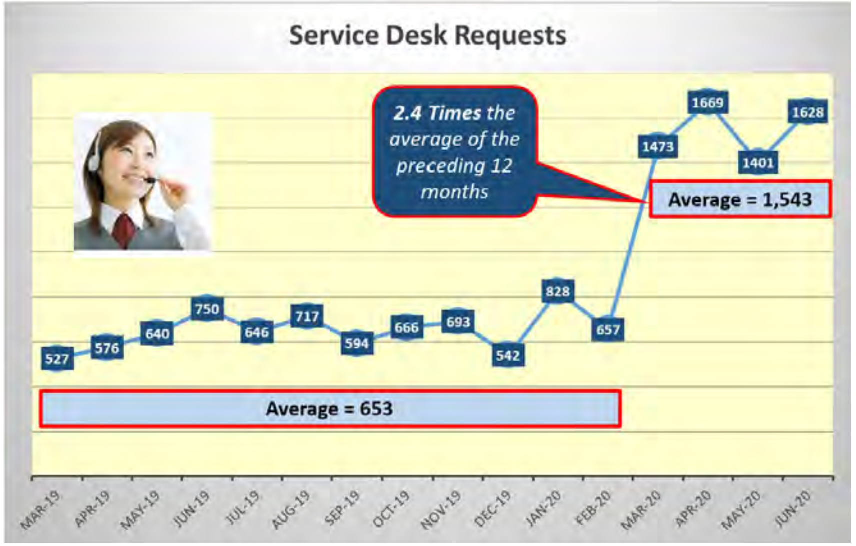
* AI/ML: artificial intelligence and machine learning

The Payoff of Sustained Enablement

Sustained enablement

“Sustained enablement” is the concept that past investments in IT *enable* future activities beyond the initial justification

- “Thank you” to the Board
- Connect the dots



COVID - 19

- Accelerated innovation
- MPI was greatly benefitted by sustained enablement in several cases – two for discussion

  Work from home (“WFH”)

  IAP Hardship withdrawal

The Payoff of Sustained Enablement

IAP Hardship Withdrawal Predicates

- Website & Mobile App
- e-Billing Replacement
  - Concurrently maintainable network; dual core switching
  - ISP – 3 load balanced providers
- Co-browsing
- Integration Platform as a Service ("iPaaS")
- Robotic Process Automation

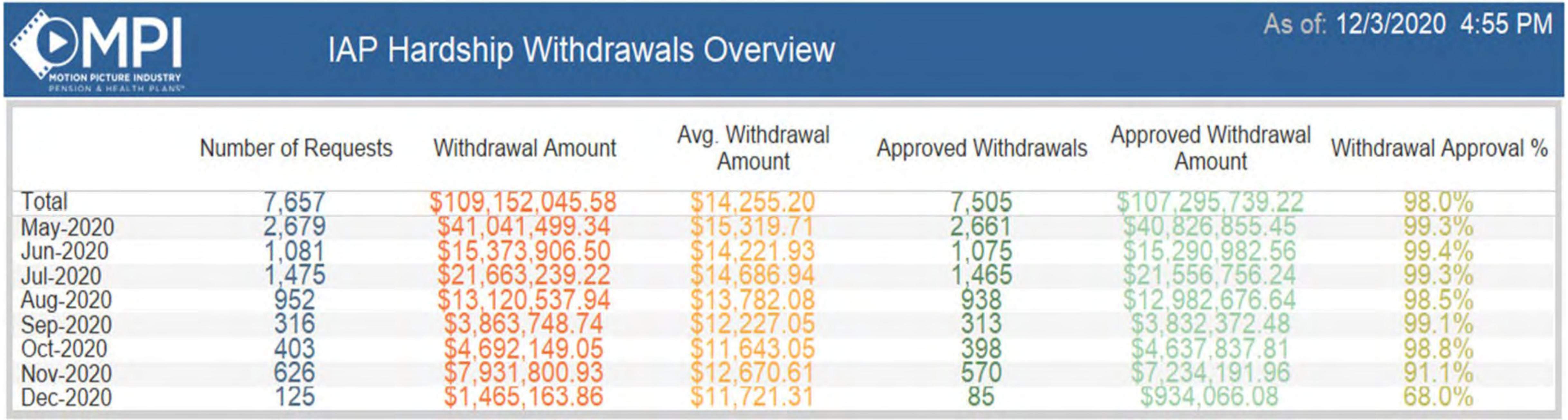
IAP Hardship Withdrawal Project

- Desktop, laptop and mobile devices
- Developed requirements
- New adaptive interview eForm
- New integration with new IICS service
  - On the fly realtime computations
  - Real time pre-population of information
- New pension system functionality
- New pension system report
- New website landing page
- Developed a new bot (RPA) to move and index IAP applications into ECM

FROM APPROVAL TO PRODUCTION IN 5 WEEKS

The Payoff of Sustained Enablement

Participants helped and funds distributed



MPI MOTION PICTURE INDUSTRY PENSION & HEALTH PLANS

IAP Hardship Withdrawals Overview

As of: 12/3/2020 4:55 PM

	Number of Requests	Withdrawal Amount	Avg. Withdrawal Amount	Approved Withdrawals	Approved Withdrawal Amount	Withdrawal Approval %
Total	7,657	$109,152,045.58	$14,255.20	7,505	$107,295,739.22	98.0%
May-2020	2,679	$41,041,499.34	$15,319.71	2,661	$40,826,855.45	99.3%
Jun-2020	1,081	$15,373,906.50	$14,221.93	1,075	$15,290,982.56	99.4%
Jul-2020	1,475	$21,663,239.22	$14,686.94	1,465	$21,556,756.24	99.3%
Aug-2020	952	$13,120,537.94	$13,782.08	938	$12,982,676.64	98.5%
Sep-2020	316	$3,863,748.74	$12,227.05	313	$3,832,372.48	99.1%
Oct-2020	403	$4,692,149.05	$11,643.05	398	$4,637,837.81	98.8%
Nov-2020	626	$7,931,800.93	$12,670.61	570	$7,234,191.96	91.1%
Dec-2020	125	$1,465,163.86	$11,721.31	85	$934,066.08	68.0%

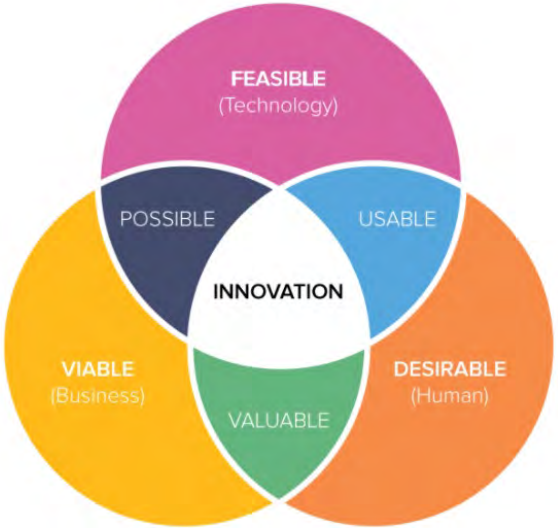
Innovation

From episodic to consistent intentionality

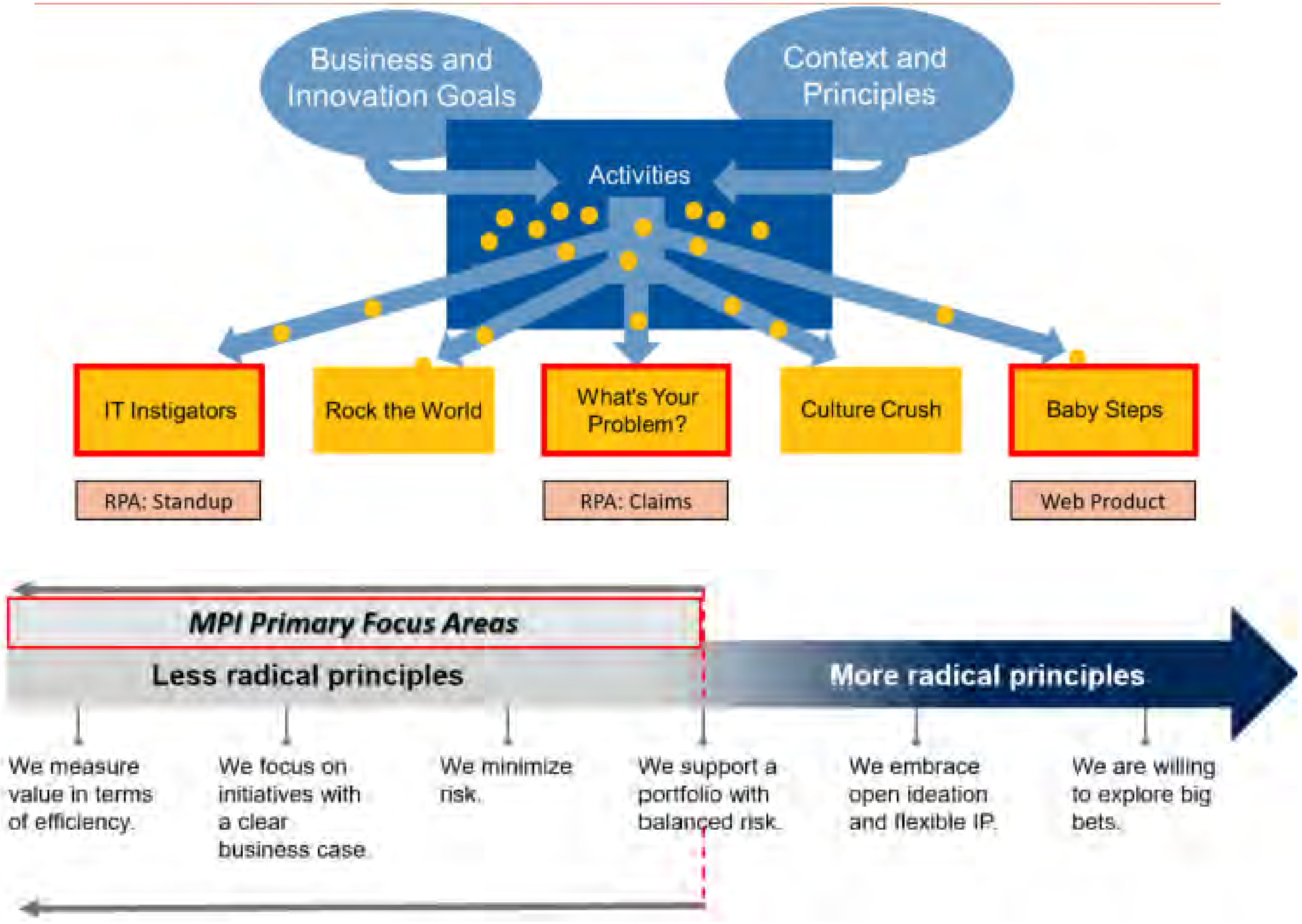
- MPI has been very innovative based on projects, e.g., iPaaS, DRaaS, RPA, questionnaire based forms, Pure storage, etc.; thus innovation has occurred episodically.
- The current intent is to operationalize it starting in IT, and later bring business leaders into the team
- “Skip level” – two reasons
  - For spreading an innovation mindset
  - For having these folks interact more with me

What is Innovation?

Innovation is the execution of new ideas that create business value.



Innovation Principles & Patterns



We measure value in terms of efficiency.

We focus on initiatives with a clear business case.

We minimize risk.

We support a portfolio with balanced risk.

We embrace open ideation and flexible IP.

We are willing to explore big bets.

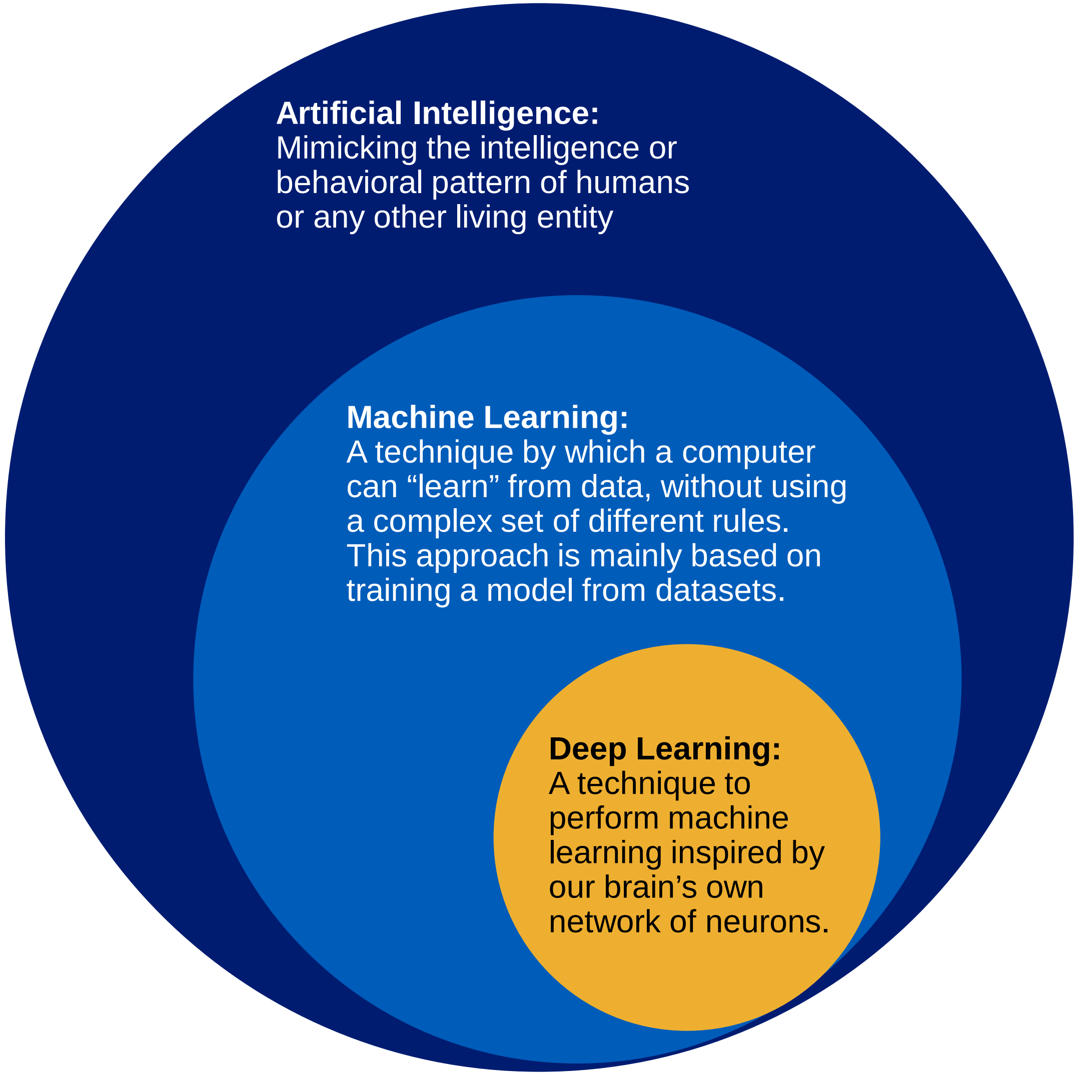
Business Goals: What Do We Want to Achieve?

Digital Business Optimization

Improved Productivity and Existing Revenue	Better Customer Experience
▪ Improve productivity ▪ Improve outcomes ▪ Get better yields	▪ Multichannel initiatives ▪ Self-service ▪ Customer service initiatives

Source: Gartner

Open AI & ChatGPT: Definitions



Artificial Intelligence: Mimicking the intelligence or behavioral pattern of humans or any other living entity

Machine Learning: A technique by which a computer can “learn” from data, without using a complex set of different rules. This approach is mainly based on training a model from datasets.

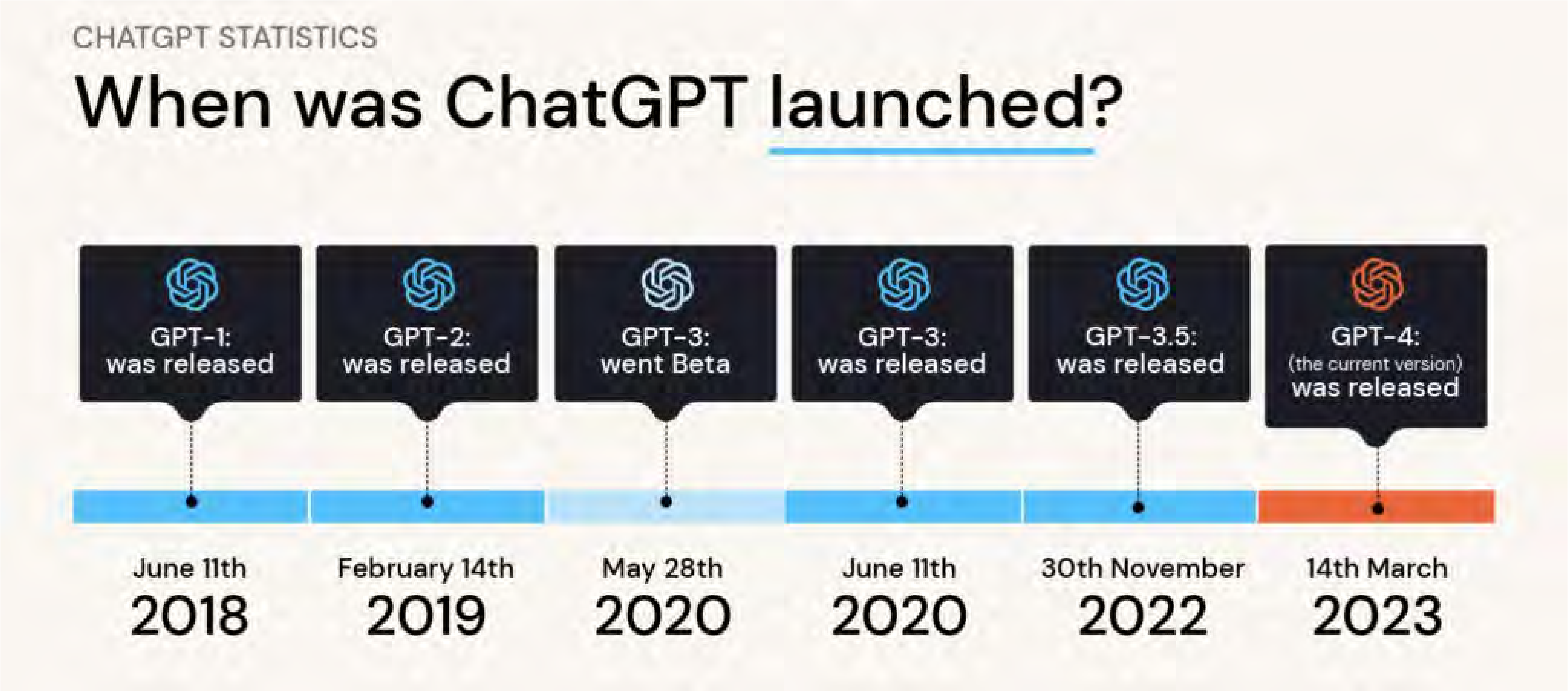
Deep Learning: A technique to perform machine learning inspired by our brain’s own network of neurons.

OpenAI is a non-profit AI research and deployment company. “Our mission is to ensure that artificial general intelligence benefits all of humanity." Funders include Peter Thiel, Elon Musk, Amazon Web Services, Infosys, YC Research and Microsoft ($1 Billion and $10 billion)

GPT (Generative Pre-trained Transformer) programming is a type of computer programming that uses deep learning algorithms to generate human-like responses to text-based prompts. It is widely used in applications such as chatbots, language translation, and content generation… Generative AI enables computers to generate brand new, original variations of content (images, video, music, speech and text) … Examples: Open AI’s ChatGPT, Google’s BERT, and Facebook’s RoBERTa.

LLM (Large Language Model) is a type of artificial intelligence algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate and predict new content.

ChatGPT Timeline



CHATGPT STATISTICS

When was ChatGPT launched?

GPT-1: was released
June 11th 2018

GPT-2: was released
February 14th 2019

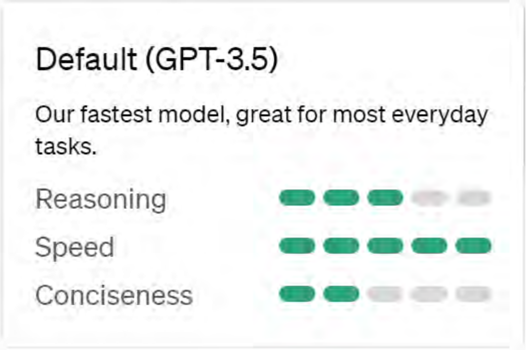
GPT-3: went Beta
May 28th 2020

GPT-3: was released
June 11th 2020

GPT-3.5: was released
30th November 2022

GPT-4: (the current version) was released
14th March 2023

175 billion parameters

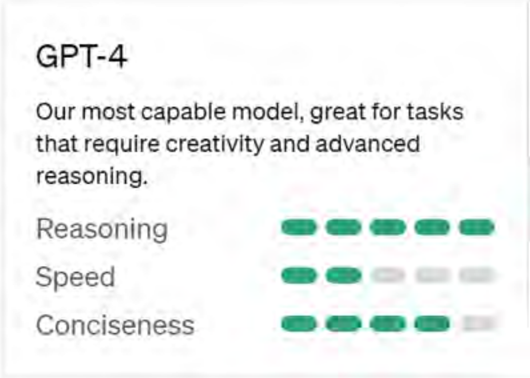


Default (GPT-3.5)

Our fastest model, great for most everyday tasks.

Reasoning	●●●○○
Speed	●●●●●
Conciseness	●●○○○

1 Trillion parameters



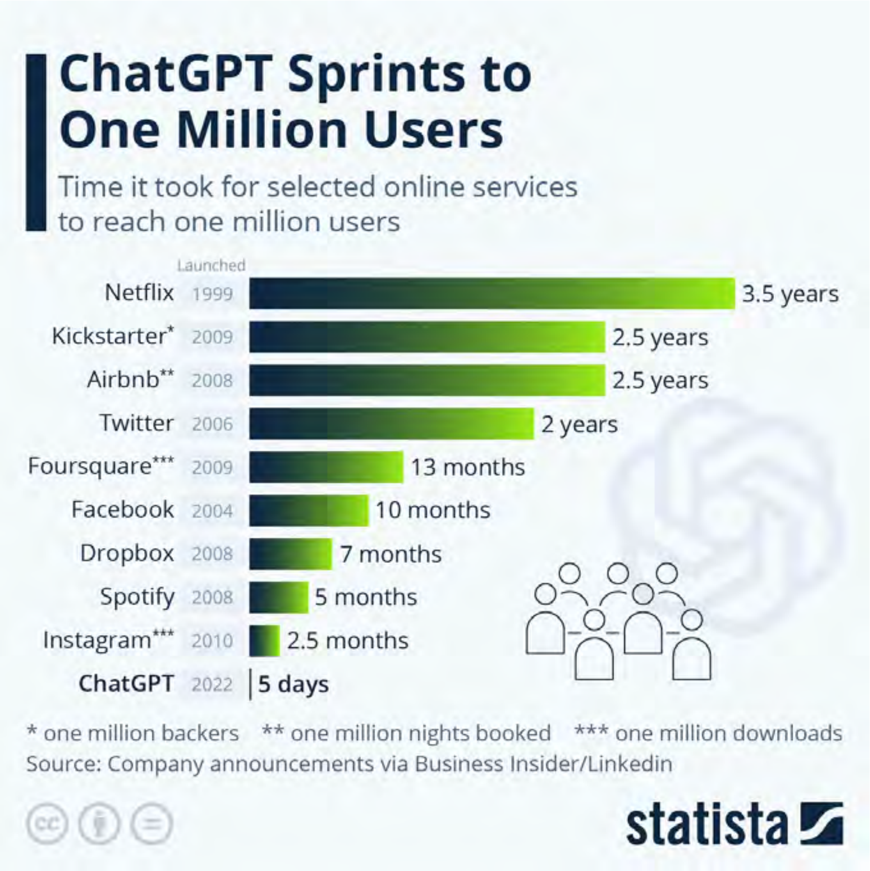
GPT-4

Our most capable model, great for tasks that require creativity and advanced reasoning.

Reasoning	●●●●●
Speed	●●○○○
Conciseness	●●●●○

Source:

Astounding Pace of Adoption: Democratizing AI



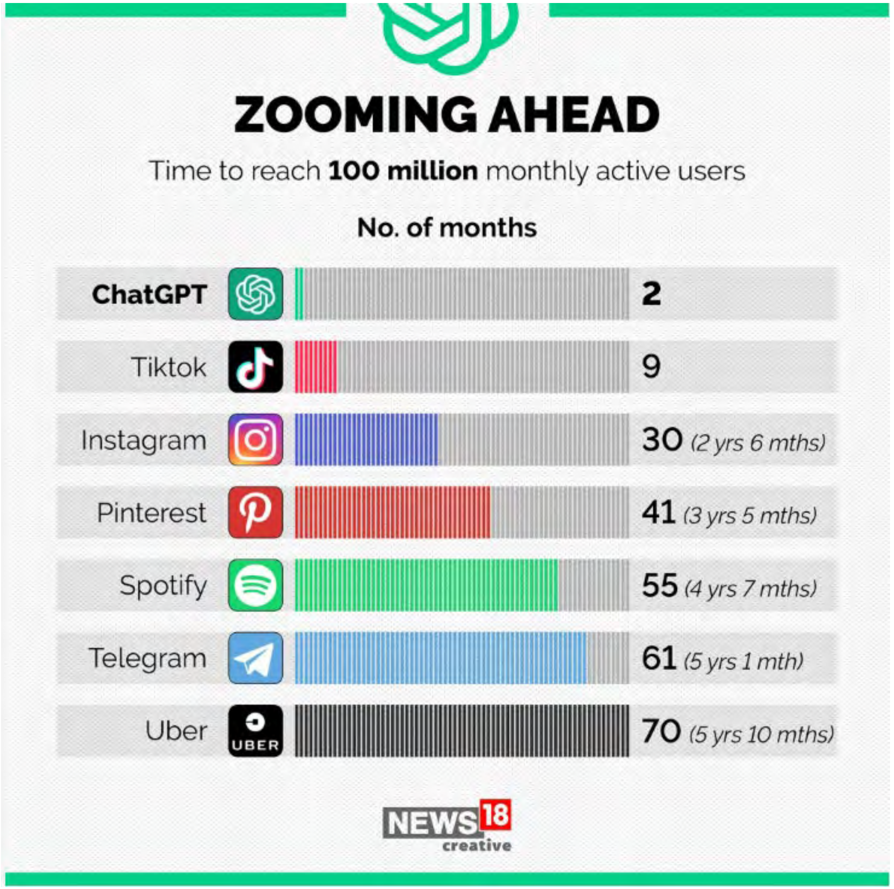
ChatGPT Sprints to One Million Users

Time it took for selected online services to reach one million users

* one million backers ** one million nights booked *** one million downloads

Source: Company announcements via Business Insider/Linkedin

statista



ZOOMING AHEAD

Time to reach **100 million** monthly active users

NEWS18 creative

ChatGPT currently has 1.16 billion users. It crossed 1 billion users in March 2023. These numbers depicted an increase of almost 55% from February 2023 to March 2023.

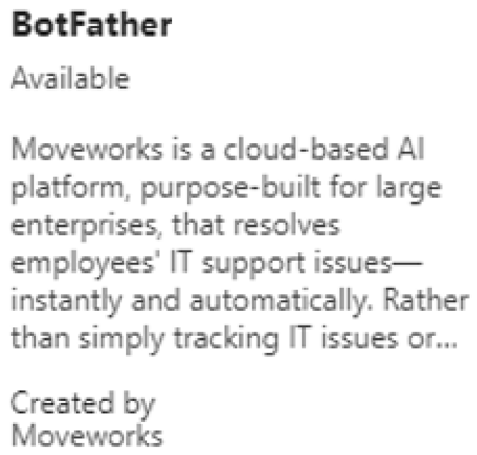
Machine Learning and Artificial Intelligence at MPI

Security Operations (M/L)

- Darktrace - Network heuristics
- Crowdstrike – Endpoint threat detection
- Palo Alto – Web firewall
- Proofpoint – Malicious email detection
- MVision (CASB) – Cloud attacks
- Microsoft Defender – Cloud anomaly detection

Security Operations (M/L)

- Pure Storage – Predictive analytics (M/L)
- ServiceDeskPlus – AI learning assistant (M/L)
- “The Botfather” – OpenAI based
  - IT Service Desk
  - PSC Answers from Knowledge Base



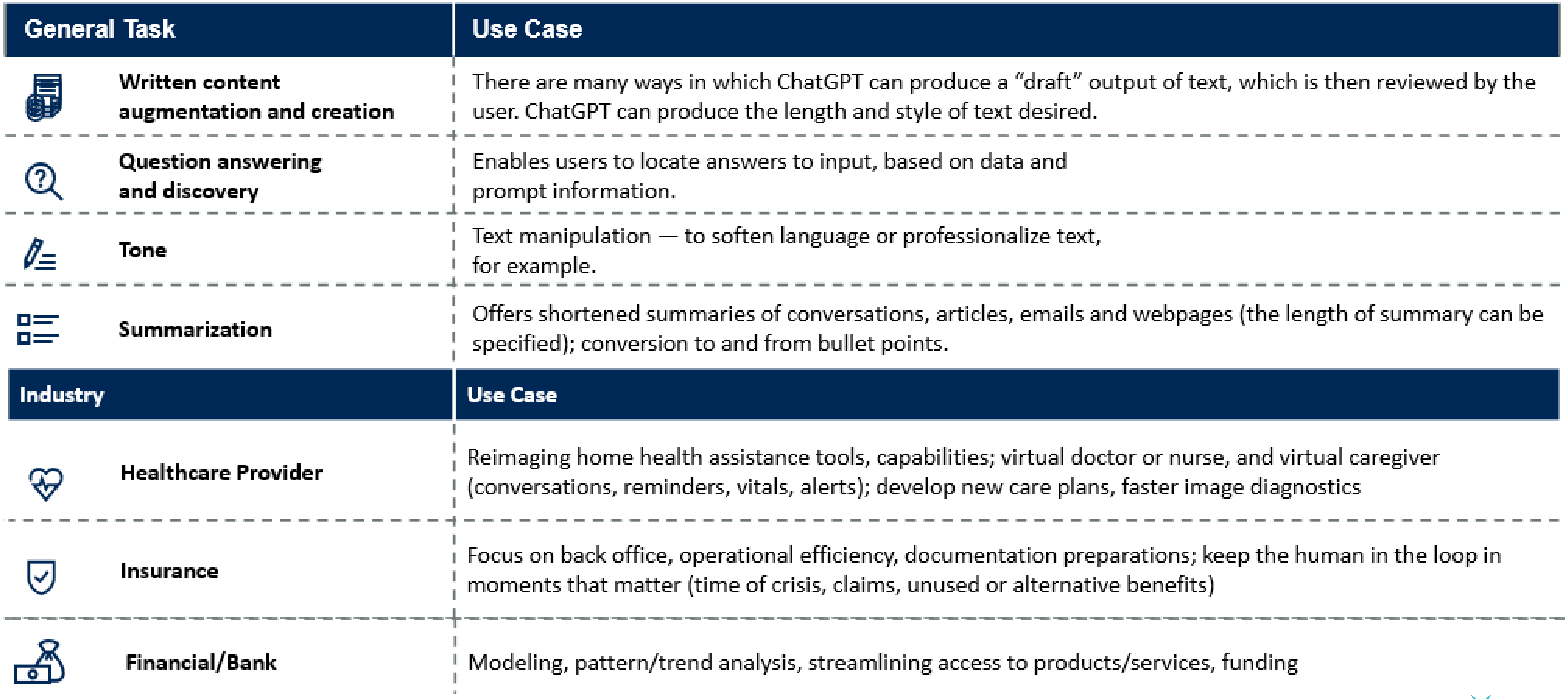
BotFather

Available

Moveworks is a cloud-based AI platform, purpose-built for large enterprises, that resolves employees' IT support issues—instantly and automatically. Rather than simply tracking IT issues or...

Created by
Moveworks

Use Cases



General Task	Use Case
Written content augmentation and creation	There are many ways in which ChatGPT can produce a "draft" output of text, which is then reviewed by the user. ChatGPT can produce the length and style of text desired.
Question answering and discovery	Enables users to locate answers to input, based on data and prompt information.
Tone	Text manipulation — to soften language or professionalize text, for example.
Summarization	Offers shortened summaries of conversations, articles, emails and webpages (the length of summary can be specified); conversion to and from bullet points.
Industry	**Use Case**
Healthcare Provider	Reimaging home health assistance tools, capabilities; virtual doctor or nurse, and virtual caregiver (conversations, reminders, vitals, alerts); develop new care plans, faster image diagnostics
Insurance	Focus on back office, operational efficiency, documentation preparations; keep the human in the loop in moments that matter (time of crisis, claims, unused or alternative benefits)
Financial/Bank	Modeling, pattern/trend analysis, streamlining access to products/services, funding

Source: Gartner Research

There is Risk

Common ChatGPT Output Risks

1. **Factual inaccuracies:** Partially true outputs that are wrong on important details.[1]
2. **Hallucinations:** Completely fabricated outputs. No actual "understanding" of content; it simply predicts text.
3. **Outdated information:** ChatGPT's "knowledge" cutoff is September 2021.
4. **Biased information:** Training data bias can result in biased outputs.[2]
5. **Copyright violations:** Outputs may resemble copyright-protected work.[3]

Source: [1] Google's AI Chatbot Bard Makes Factual Error in First Demo, The Verge; [2] ChatGPT Writes Job Posts, Textio; [3] AI Art Tools Stable Diffusion and Midjourney Targeted With Copyright Lawsuit, The Verge

GPT Labor Market Impact

Out of **10 U.S. workers**

10% OF WORK IMPACTED

Six workers will have at least **10%** of their work tasks impacted by GPT technology

50% OF WORK IMPACTED

Two workers will have over **50%** of their work tasks impacted by GPT

What makes **your** job exposed to GPT?

Exposure: potential economic impact

● Low Exposure

- Low wages
- Manufacturing
- Agriculture
- Mining
- Jobs requiring low formal education
- Jobs requiring many hours of on-the-job training
- Critical thinking Skills
- Science skills

● High Exposure

- High wages
- Writing
- Programming
- Information processing
- Work that requires college degree or higher
- Minimal on-the-job training
- Routine & repetitive work

What **jobs** are exposed to GPT?

● Low Exposure

- Athletes
- Automotive Repairers
- Cement Masons
- Cooks
- Pile Driver Operators
- Stonemasons
- Tire Repairers and Changers
- Dishwashers
- Carpenter Helpers

● High Exposure

- Interpreters + Translators
- Survey Researchers
- Writers and Authors
- Public Relations Specialists
- Tax Preparers
- Mathematicians
- Blockchain Engineers
- Proofreaders and Copy Markers
- Accountants and Auditors

OpenAI's Recommendation for Government Focus

- Prepare for economic disruption
- Reform education policy
- Reform worker training policy
- Reform safety net programs

Source: OpenAI

Report: "An early look at the Labour Market Impact of Large Language Models" - March 21 2023

Designed by: Harrison Schell

Source: OpenAI Research

“Co-pilots”: Emergence and Arms Race

Co-pilot is software enabling simultaneous querying of multiple applications through spoken (or typed) language which, using Large Language Models, generates transformed output. (Joel’s definition)

Microsoft will be releasing its copilot in July. It will be imbedded in all of it office productivity tools, including Word, Excel, PowePoint, Outlook, Teams and PowerBI… It will enable profound changes for knowledge workers.

For example, you’ll be able to say, “please generate an eight slide board level presentation explaining artificial intelligence, machine learning, large language models and how these technologies interact to generate transformed content. Also Include how this will affect knowledge workers in the future.”

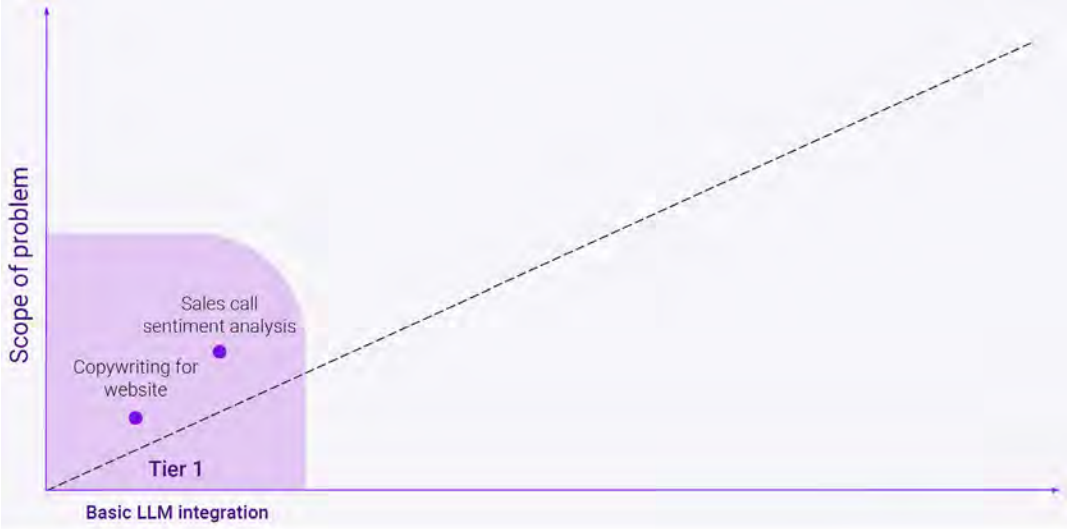
“ Today marks the next major step in the evolution of how we interact with computing which will fundamentally change the way we work and unlock a new wave of productivity growth,” said **Satya Nadella, Chairman and CEO, Microsoft.** “With our new copilot for work, we’re giving people more agency and making technology more accessible through the most universal interface — natural language. ”

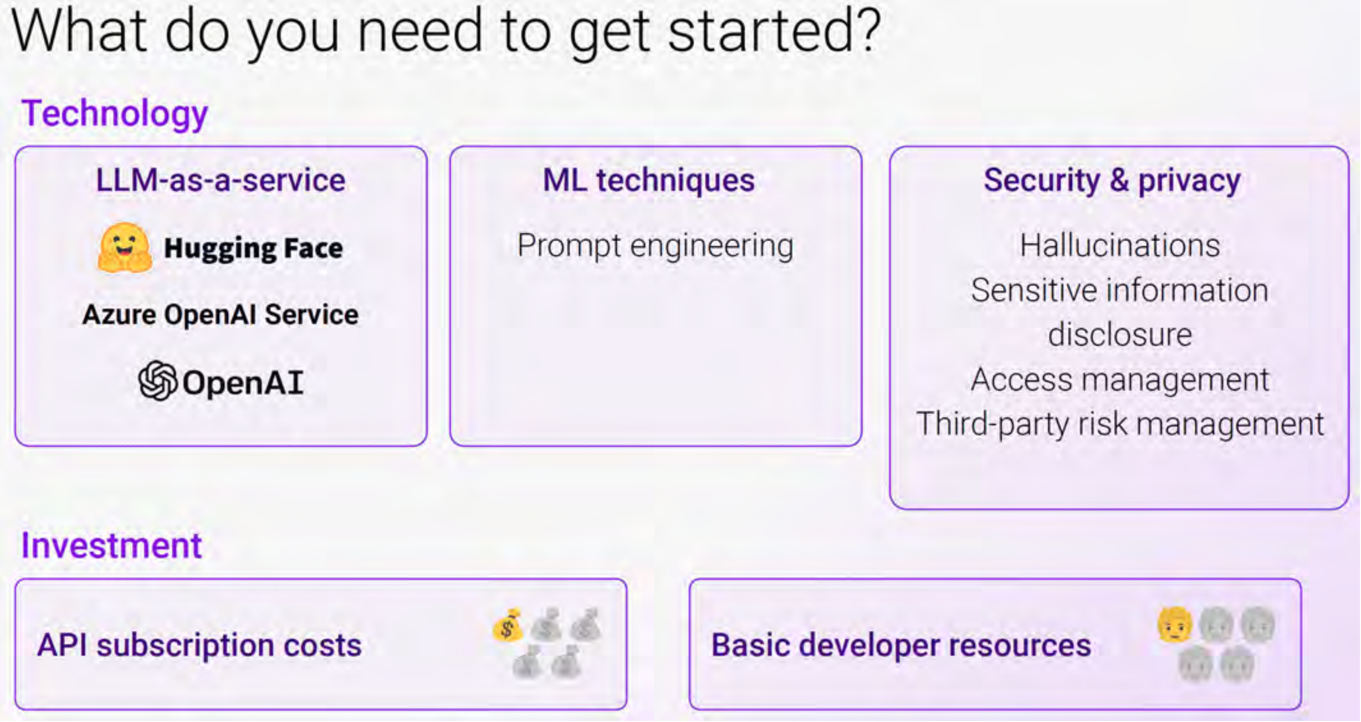
RECOMMENDED VIDEO: *Microsoft's AI Future of Work Event: Everything Revealed in 8 Minutes*

https://www.youtube.com/watch?v=VqhDnaqhnd4

“Co-pilots”: Tier 1 Basic LLM Integration

Moveworks





What do you need to get started?

Technology

LLM-as-a-service

Hugging Face

Azure OpenAI Service

OpenAI

ML techniques

Prompt engineering

Security & privacy

Hallucinations
Sensitive information disclosure
Access management
Third-party risk management

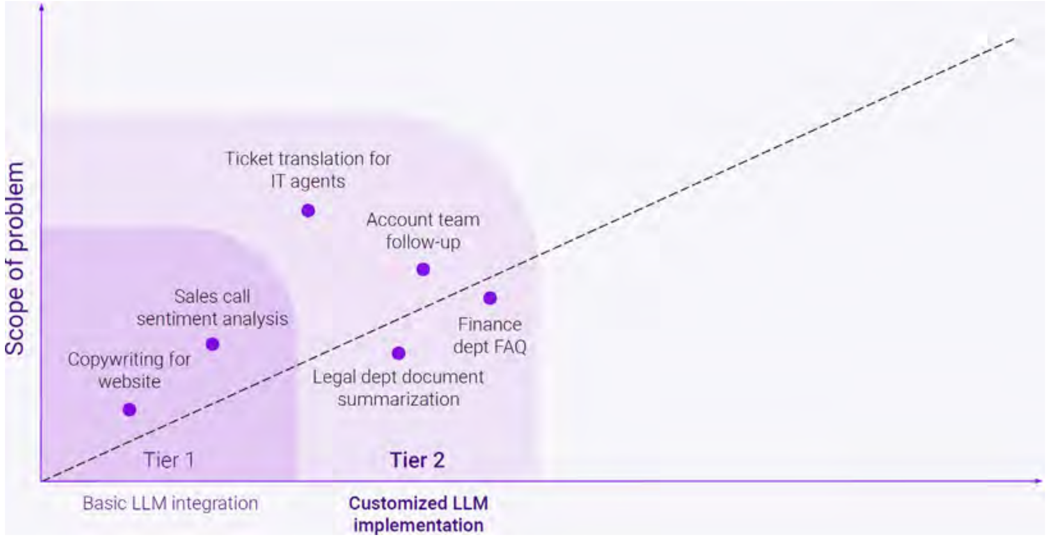
Investment

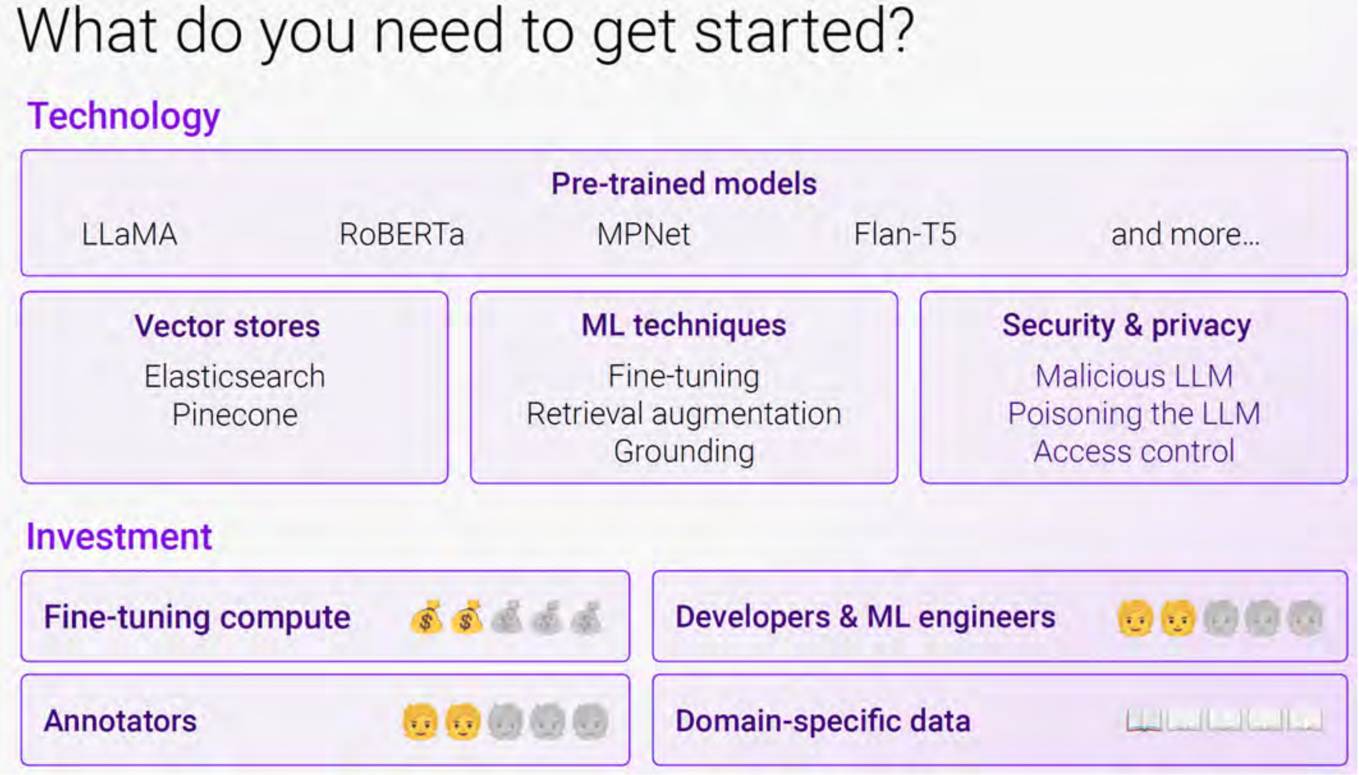
API subscription costs 💰💰💰💰💰

Basic developer resources 🧑🧑🧑🧑🧑

“Co-pilots”: Tier 2 Customized LLM Implementation

Moveworks





What do you need to get started?

Technology

Pre-trained models

LLaMA RoBERTa MPNet Flan-T5 and more...

Vector stores	**ML techniques**	**Security & privacy**
Elasticsearch Pinecone	Fine-tuning Retrieval augmentation Grounding	Malicious LLM Poisoning the LLM Access control

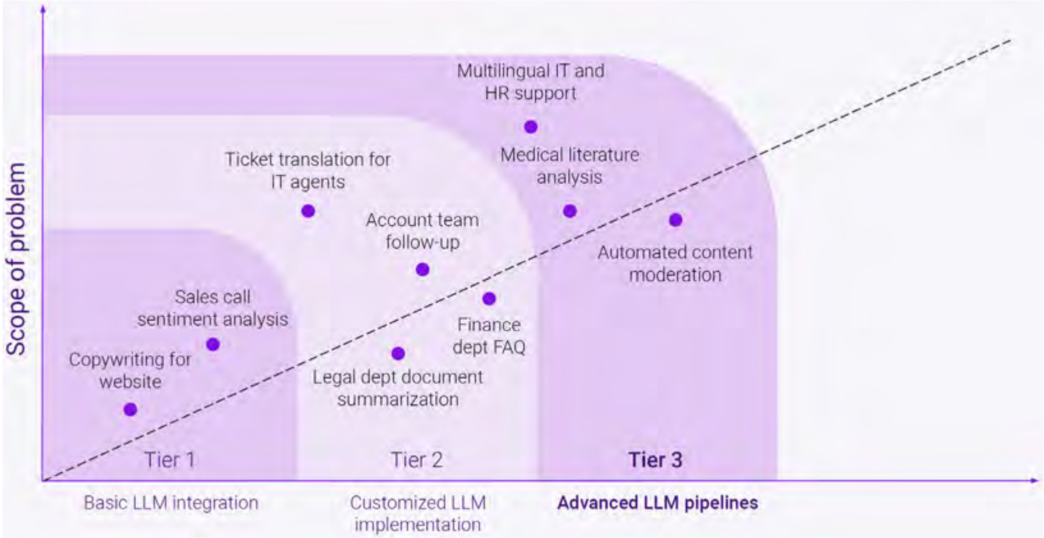
Investment

Fine-tuning compute	●●○○○	**Developers & ML engineers**	●●○○○
Annotators	●●○○○	**Domain-specific data**	●○○○○

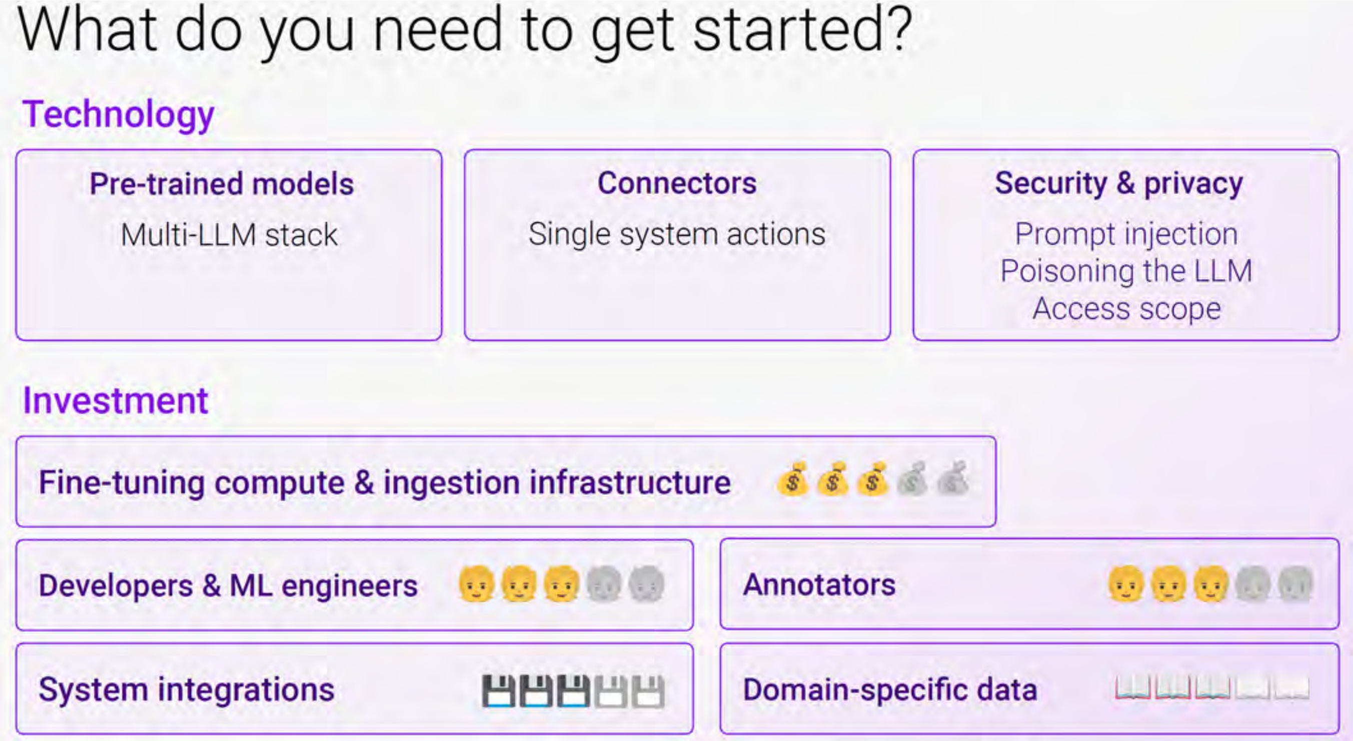
Tier 2 copilots solve domain-specific problems

"Co-pilots": Tier 3 Advanced LLM Pipelines

Moveworks



Scope of problem
Multilingual IT and HR support
Medical literature analysis
Ticket translation for IT agents
Account team follow-up
Automated content moderation
Sales call sentiment analysis
Finance dept FAQ
Copywriting for website
Legal dept document summarization
Tier 1
Tier 2
Tier 3
Basic LLM integration
Customized LLM implementation
Advanced LLM pipelines



What do you need to get started?

Technology

Pre-trained models
Multi-LLM stack

Connectors
Single system actions

Security & privacy
Prompt injection
Poisoning the LLM
Access scope

Investment

Fine-tuning compute & ingestion infrastructure ●●●○○

Developers & ML engineers ●●●○○

Annotators ●●●○○

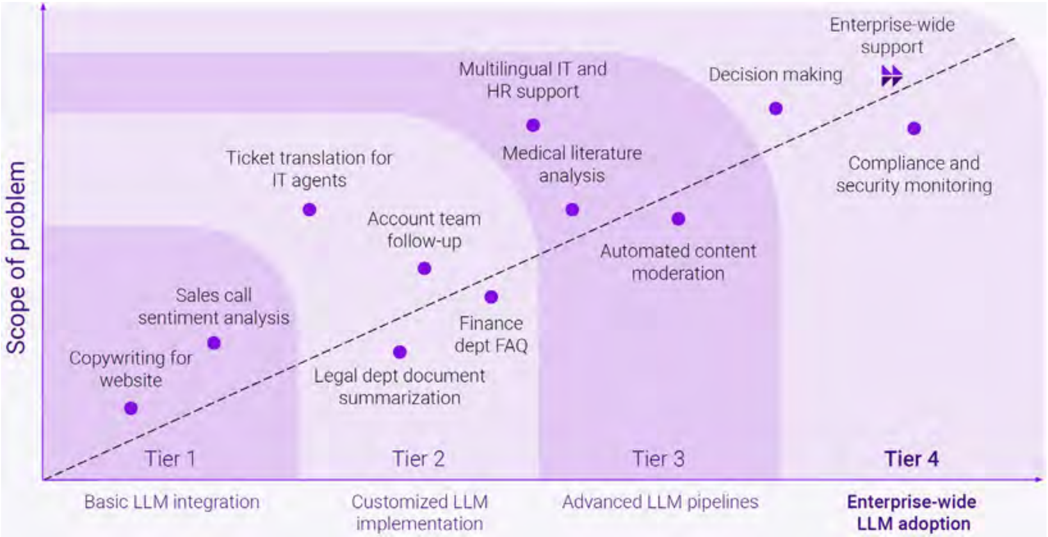
System integrations ●●●○○

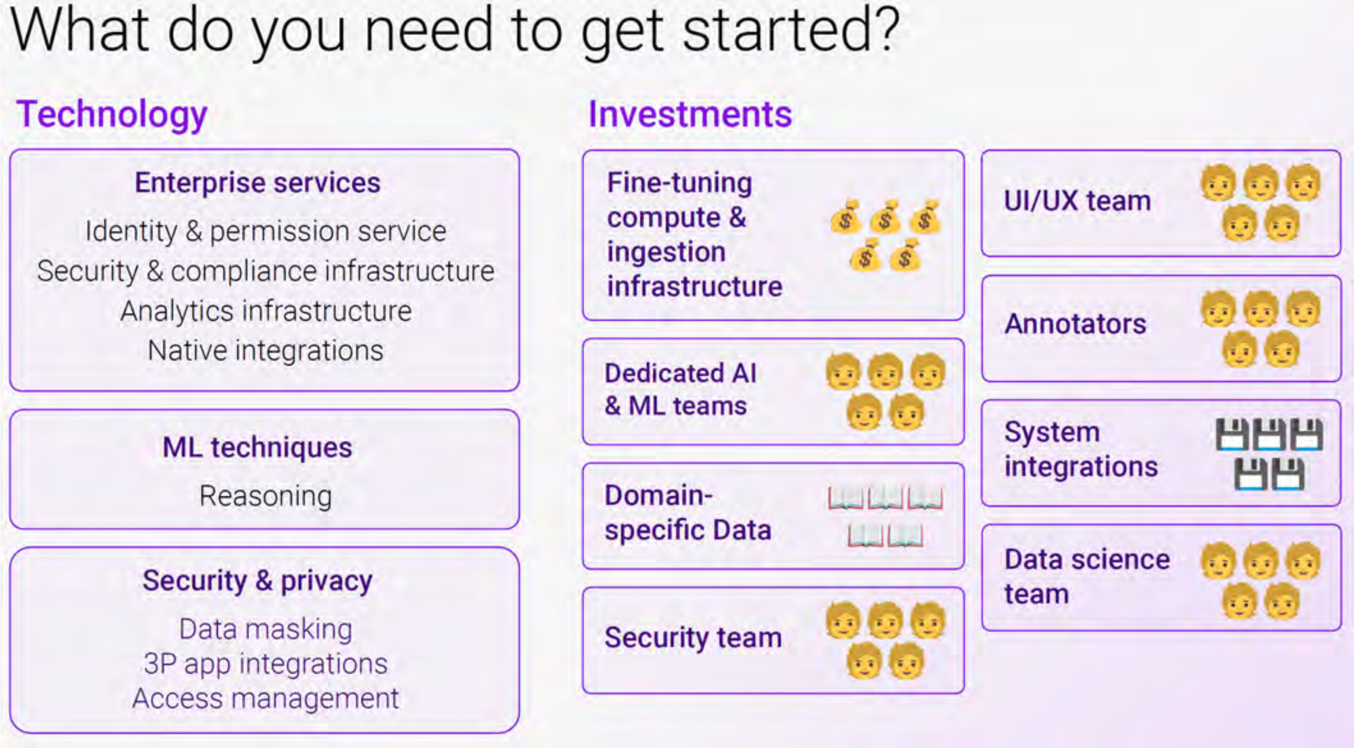
Domain-specific data ●●●○○

Tier 3 copilots use a stack of LLMs across depts

“Co-pilots”: Tier 4 Enterprise–wide LLM Adoption

Moveworks





What do you need to get started?

Technology

Enterprise services

Identity & permission service
Security & compliance infrastructure
Analytics infrastructure
Native integrations

ML techniques

Reasoning

Security & privacy

Data masking
3P app integrations
Access management

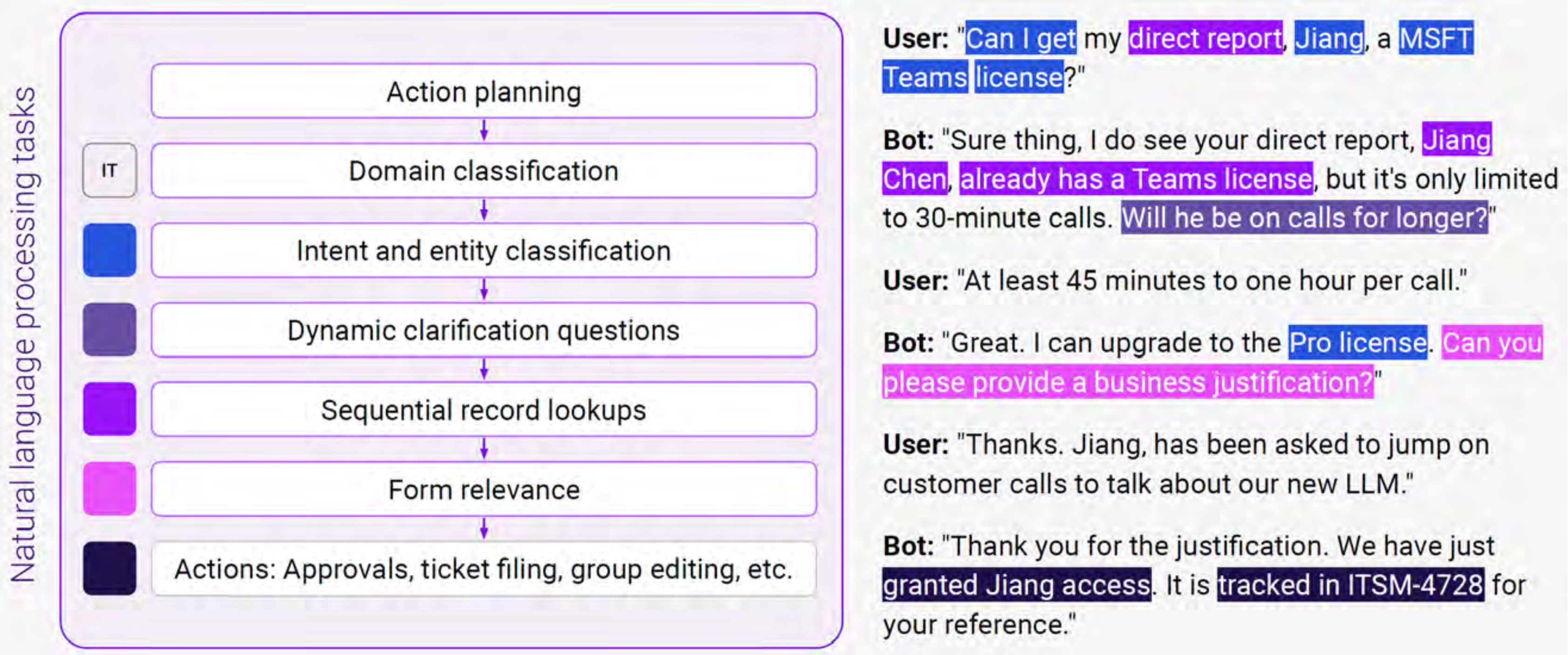
Investments

- Fine-tuning compute & ingestion infrastructure
- Dedicated AI & ML teams
- Domain-specific Data
- Security team
- UI/UX team
- Annotators
- System integrations
- Data science team

Tier 4 copilots solve enterprise-wide problems

"Co-pilots": Even Task Level Precision is Difficult

Moveworks


Natural language processing tasks
Action planning
IT
Domain classification
Intent and entity classification
Dynamic clarification questions
Sequential record lookups
Form relevance
Actions: Approvals, ticket filing, group editing, etc.

User: "Can I get my direct report, Jiang, a MSFT Teams license?"

Bot: "Sure thing, I do see your direct report, Jiang Chen, already has a Teams license, but it's only limited to 30-minute calls. Will he be on calls for longer?"

User: "At least 45 minutes to one hour per call."

Bot: "Great. I can upgrade to the Pro license. Can you please provide a business justification?"

User: "Thanks. Jiang, has been asked to jump on customer calls to talk about our new LLM."

Bot: "Thank you for the justification. We have just granted Jiang access. It is tracked in ITSM-4728 for your reference."

The morale of the story:

This is complicated, needs multi-disciplined technical experts and it is expensive. The best path for us is to buy from expert companies.

Takeaways

PSCBD (I’ll explain later)

Organizational Maturity: Project → Program → Product

Digital Transformation: Multifaceted, organization defined, near infinite possibilities

Machine Learning, Artificial Intelligence, Generative Pre-Trained Transformer: Don’t go it alone

Questions?

Thank You

For more info, please contact

Joel Manfredo
Chief Information, Innovation
& Digital Officer, Motion Picture
Industry Pension & Health Plans

jmanfredo@mpiphp.org

818.769.0007 Ext 2400

Multiemployer IT Summit

What's NExT?

Prepare for Your Next Cyber Renewal

Matthew Jackson, SVP,
Segal Select Insurance

Scott Schreiber, Technical Project Manager,
Premier Technology Solutions, Inc.

October 10-11, 2023 / San Diego

Proudly sponsored by

Segal

Agenda

1. State of the Cyber Insurance Market
2. Insurance for Social Engineering Fraud
3. Cyber Insurance Application Process
4. Preparing for your Next Renewal
5. Questions

State of the Cyber Insurance Market

01

There remains an onus on Insureds for minimum/base controls

Including: implementation of MFA; Secure RDP’s; robust backup procedures, training and Incident Response Plans

02

Rate increases have slowed

More stability in premiums, including some decreases

03

Broader Terms/Conditions

Reduction/removal of co-insurance; lower retentions; and increase in sublimits

04

Increase in Cyber Liability Capacity YOY

Existing markets increase capacity as well as the introduction of additional market capacity

State of the Cyber Insurance Market

05

Increase in automatic renewals

Automatic renewals can still include changes to premium and terms, but no application requirement usually seen as a positive

06

Inconsistency with admitted/non-admitted markets still exists

Many carriers continue to use non-admitted paper to allow greater flexibility on rate and coverage changes

07

Move towards universal applications

Still evolving. Limited flexibility on terms

08

Interest in additional products/limits

Increased purchasing of Excess Social Engineering Fraud coverage

Insurance for Social Engineering Fraud

Attacks are generally covered by most carriers when malware is added, data is stolen or held hostage, or money transferred:

- The coverage may have exclusions and require certain procedures to be followed in order to have a covered claim (independent call back provisions, etc.)
- If money is stolen, standard coverage limits are often sublimited to between $50K and $250K regardless of the full policy limit
- There may be similar coverage in other policies such as a fidelity bond
- Larger coverage limits are usually only available by having excess carriers participate in a program

Insurance for Social Engineering Fraud

Standalone excess policies available for social engineering fraud

- Typical attachment point of $250,000;
- Requested limits are usually $1-million to $5-million;
- Appetite can depend on which carrier writes primary

Insurance for Social Engineering Fraud

Key Application Questions

- Average volume and frequency of fund transfers over last 12 months, largest to totals? Domestic and foreign
- Anti-fraud training for detection of phishing and social engineering scams?
- Do you authenticate vendor instructions?
- Who is authorized to direct accounts payable to pay an invoice and authenticate instructions in place?
- Authority on wire transfers, verbally, in writing and banking instructions?

Cyber Insurance Application Process

- How long is the application process?
  - What information is needed?
  - How complex is the application?
  - What are key differences between carrier applications?
- Key application questions
- Sample responses
- What happens if required technology has not been implemented?
- Case studies/impacts to coverage terms and costs

Third Party Network Scans

Cyber liability insurance carriers relying more on third party networks scans:

- Bitsight
- CyRisk Insight Engine
- In-house proprietary scans

Mixed feedback from clients

- Scanning wrong urls (e.g., union’s site rather than fund’s site);
- Outdated scans

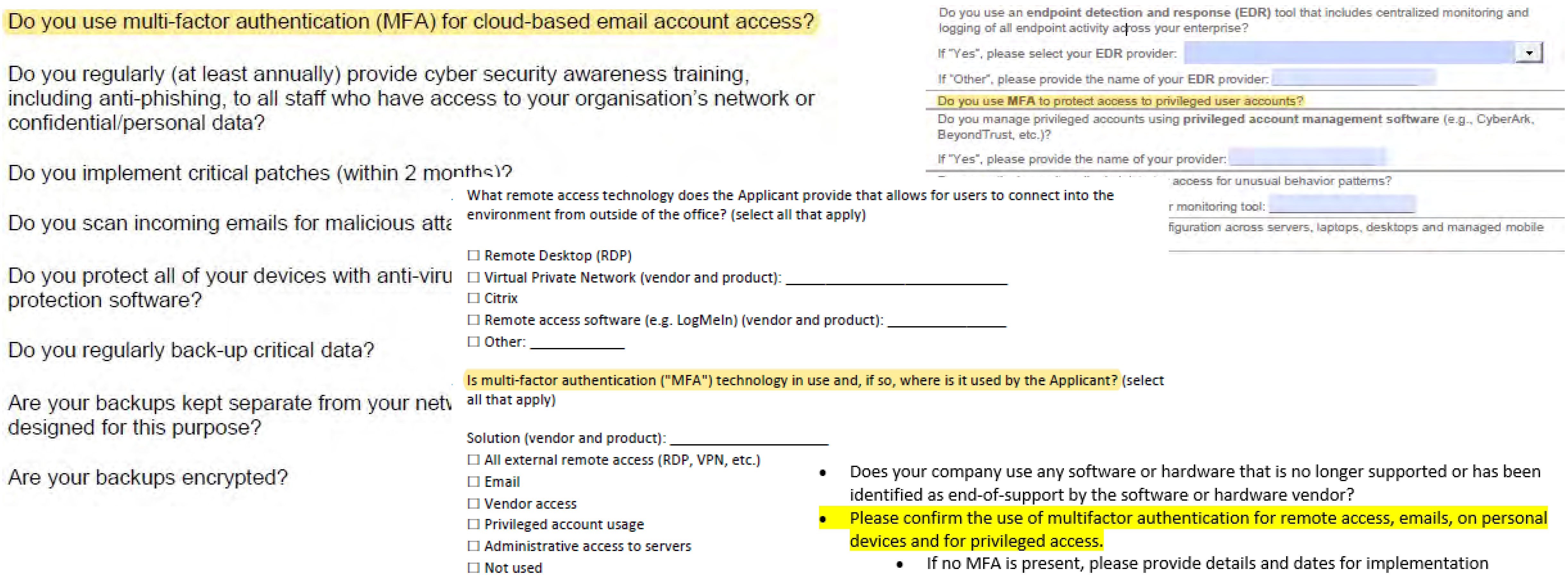
Scans done periodically throughout the year

May require response midterm or prior to next renewal

Beware Warranty Statements

- In general, warranty statements are very broad attestations that the proposed insureds are not aware of any incident, act, knowledge, error, or omission which might result in a claim under the policy
- Usually required for first year of coverage, but an important factor when applying for renewals and considering changing carriers
- Disputes can arise with the insurance company regarding the knowledge that may lead to insurance claim denials or even policy recession by the carrier

Sample MFA Questions



Do you use multi-factor authentication (MFA) for cloud-based email account access?

Do you regularly (at least annually) provide cyber security awareness training, including anti-phishing, to all staff who have access to your organisation's network or confidential/personal data?

Do you implement critical patches (within 2 months)?

Do you scan incoming emails for malicious atta

Do you protect all of your devices with anti-viru protection software?

Do you regularly back-up critical data?

Are your backups kept separate from your netw designed for this purpose?

Are your backups encrypted?

Do you use an **endpoint detection and response (EDR)** tool that includes centralized monitoring and logging of all endpoint activity across your enterprise?

If "Yes", please select your EDR provider:

If "Other", please provide the name of your EDR provider:

Do you use **MFA** to protect access to privileged user accounts?

Do you manage privileged accounts using **privileged account management software** (e.g., CyberArk, BeyondTrust, etc.)?

If "Yes", please provide the name of your provider:

access for unusual behavior patterns?

r monitoring tool:

figuration across servers, laptops, desktops and managed mobile

What remote access technology does the Applicant provide that allows for users to connect into the environment from outside of the office? (select all that apply)

☐ Remote Desktop (RDP)
☐ Virtual Private Network (vendor and product): ______________________________
☐ Citrix
☐ Remote access software (e.g. LogMeIn) (vendor and product): ________________
☐ Other: ____________

Is multi-factor authentication ("MFA") technology in use and, if so, where is it used by the Applicant? (select all that apply)

Solution (vendor and product): ____________________
☐ All external remote access (RDP, VPN, etc.)
☐ Email
☐ Vendor access
☐ Privileged account usage
☐ Administrative access to servers
☐ Not used

- Does your company use any software or hardware that is no longer supported or has been identified as end-of-support by the software or hardware vendor?
- Please confirm the use of multifactor authentication for remote access, emails, on personal devices and for privileged access.
  - If no MFA is present, please provide details and dates for implementation

Preparing For Your Next Renewal

Cybersecurity Measures They Look For

Endpoint detection and response tools, MFA, email filtering, regular employee training, patching and updating

- EDR- Microsoft Defender P2, Crowdstrike, Rapid7, SentinelOne
  - Cost: As low as $5/user/mo
- Email filtering tools such as O365, Proofpoint, Mimecast, Barracuda will help to eliminate junk, spam and spoofed emails
  - Cost: As low as $3/user/mo
- Employee Training. This should include Phishing Campaigns
  - Cost: $5-7/user/mo
    - 59% of users can’t spot phishing,
    - 94% of attacks happen through email
- Patching and Updates are practically free! You just need a process

Cost Is Driven by the Amount of Exposure

Consider Expanding Your Security Footprint

- Network Scans are becoming cheaper and easier; External, Internal, AD, Penetration
  - Unlimited Vulnerability scan cost: $200-$500/mo
  - Unlimited AD scan cost: $200-$500/mo
- Security Information Event Monitoring (SIEM)
  - Cost $30/user/mo
- Dark Web Monitoring
  - Cost: $150/mo

Consider Implementing Privileged Identity Management with Azure P2

- Minimize access to secure information or resources
  - Provides Just-in-time, time-bound, approval, notifications etc.
- Risk-based user sign-in protection
  - Impossible travel, anonymous IP addresses, unfamiliar locations etc.

Consider Expanding Your Policies and Procedures

- Incident Response Plan
  - Cost: Free
- Disaster Recovery
- Business Continuity
- Etc.

Not Sure Where Your Gaps Are?

Have an IT Review done to know where you can go and how to get there

- Cost: Dependent on infrastructure.

Questions?

Thank You

**For more info,
please contact us**

Scott Schreiber
sschreiber@premiertechnolgoy.com
212.576.1602

Matthew Jackson
mjackson@segalco.com
212.251.5387