National Institute of BUILDING SCIENCES™

Webinar: Collaborative Digital Delivery in the Age of Information Privacy and Cybersecurity

JUN 1, 2022 | 1:30 PM – 3:00 PM ET

WELCOME AND SPONSOR INTRO

Meet the NIBS BIM Council and our Sponsors

Roger Grant, FbSI

Executive Director Building Information Management | National Institute of Building Sciences

National Institute of BUILDING SCIENCES™

THANK YOU TO OUR SPONSORS

COMPASS datacenters®

AUTODESK

dRofus
A NEMETSCHEK COMPANY

bsi.

NEWFORMA.

Building Information Management Council

MODERATORS

Rachel Riopel, AIA
Digital Practice Leader, HDR
Chair of NIBS BIM Council BOD

Brok Howard
Product Manager, dRofus

Connor Christian, PE
Product Manager, Procore Technologies

Nathan C. Wood
Executive Director, CPC

KEY CONTRIBUTORS

Rahul Shah
Sector Development Director, BSI Group Inc

Dr. Ivan Panushev
Principal Partner Solutions Architect for Engineering, Construction, and Real Estate, AWS

Johnny Fortune
BIM Manager, PRIME AE Group

Wanda Lenkewich
CEO, Chinook Systems Inc.

KEY CONTRIBUTORS

Lynn Burns
ISSM & FSO, HDR Inc.

Carrie Sturts Dossick, P.E.
Professor of Construction Management, Associate Dean of Research, College of Built Environments, UW

Robert "Bobby" Prostko
Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion

Alexandria Luck
Fellow, the Institution of Civil Engineers

NIBS BIM PROGRAM

NIBS
(Board of Directors)

U.S. National BIM Program

BIM Program Partners
(Steering Committee)

BIM Council
(Board of Direction)

NBP Workstreams

- Owner Adoption
- Project Delivery Implementation
- Stakeholder Engagement
- Standards and Guidelines
- Education and Training
- Legal and Insurance

U.S. National BIM Standard (NBIMS)

- **NBIMS-US Project Committee**
- **NBIMS-US Planning Committee**
- **NBIMS-US Content Workgroups**
  - CORE BIM Workgroups
  - BIM Execution Planning
  - BIM Use Definitions
  - Information Standards
  - COBie
  - Additional under consideration

U.S. National CAD Standard (NCS)

- **NCS Steering Committee**
- **Task Teams**

www.nibs.org/BIMC

www.nibs.org/projects/national-bim-program

PROGRAM VISION

To accelerate the digital transformation of the built asset industry to achieve optimal economic, environmental, and functional performance of our US built environment.

PROGRAM MISSION

To transform lifecycle information management practices by creating and advancing the consistent adoption of next-generation information management standards and practices to significantly improve the built environment delivery and operations processes.

LEARNING OBJECTIVES

WHAT ARE WE HERE TO LEARN?

Information on receiving Learning Units for today's webinar will be emailed to you after the session.

Current Standards

Identify current standards and requirements related to information privacy and cybersecurity as it relates to the built environment.

Data Privacy

Recognize and state 1-2 key impacts of information privacy and cybersecurity requirements to the collaborative digital delivery process.

Technology Evolution

Explain how technology has evolved in support of collaborative digital delivery.

Impacts to Process

Identify 3 process areas impacted by requirements supporting information privacy and cybersecurity.

In-Session Polling Instructions

To engage everyone, we will be using a polling application called: Mentimeter!

Here's how it works:

1. Scan the code to the right (using your phone)
2. Answer this first question as a trial run
3. Listen for cues to share your feedback throughout the presentation

The results from today's surveys will be used in follow up work sessions.

National Institute of BUILDING SCIENCES™

Webinar: Collaborative Digital Delivery in the Age of Information Privacy and Cybersecurity

JUN 1, 2022 | 1:30 PM – 3:00 PM ET

AGENDA

01 WHY NOW?
02 TECHNOLOGY
03 PEOPLE
04 PROCESS
05 NATIONAL STANDARDS
06 WRAP

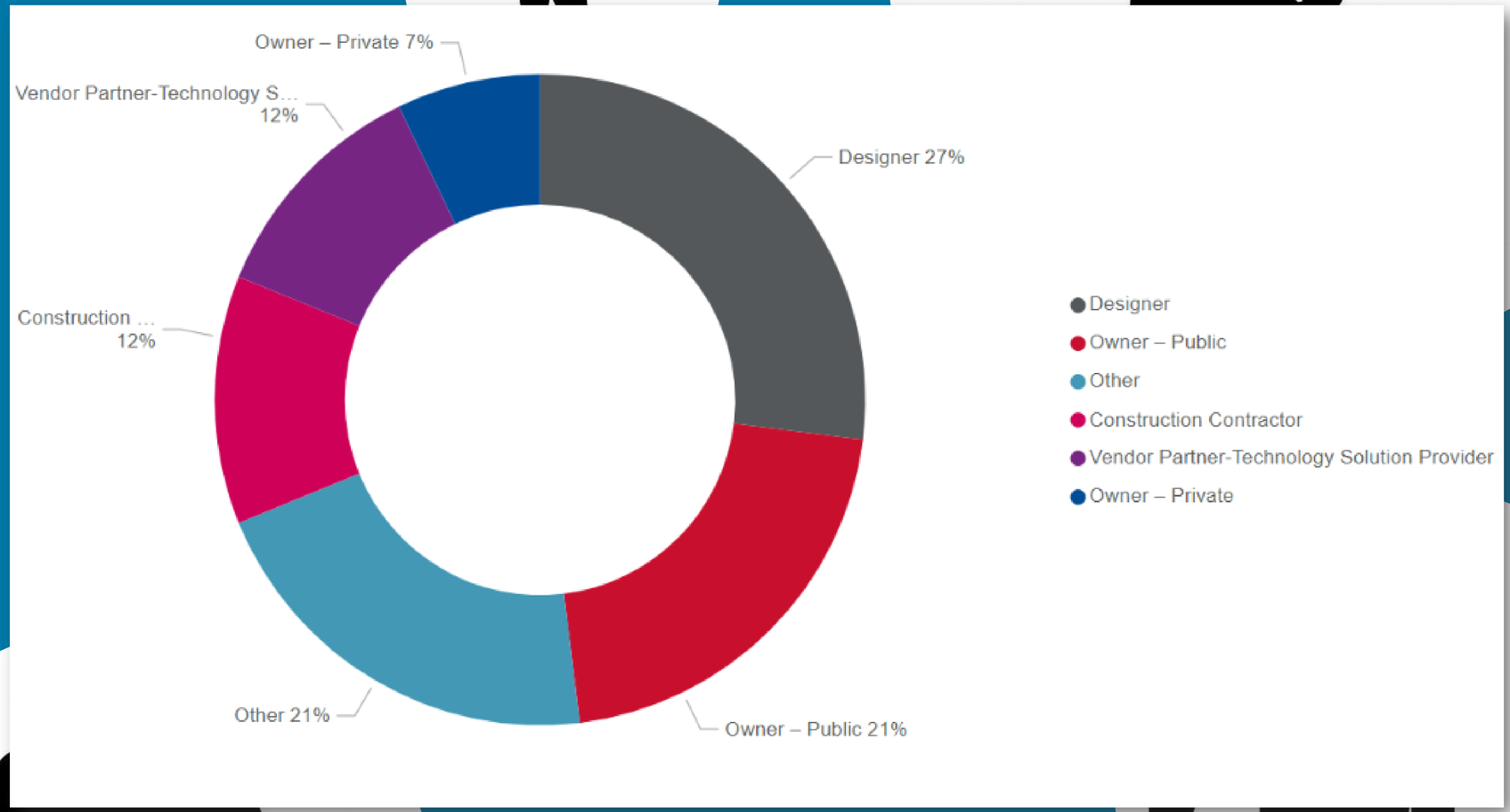
WHY NOW?

Stakeholders and the status quo

Rachel Riopel, AIA
Digital Practice Leader | HDR Inc.
BIM Council Chair

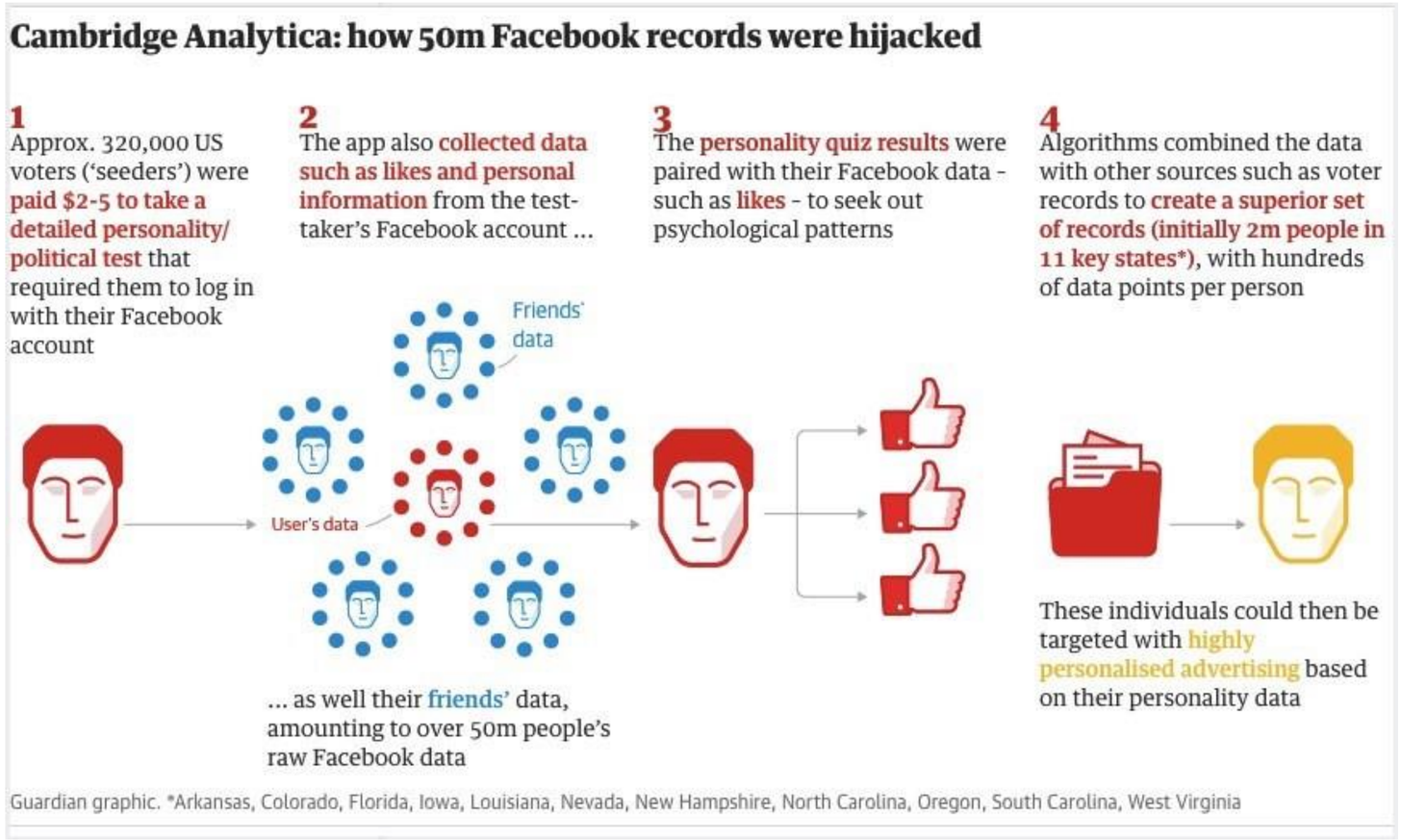
Stakeholder Perspectives

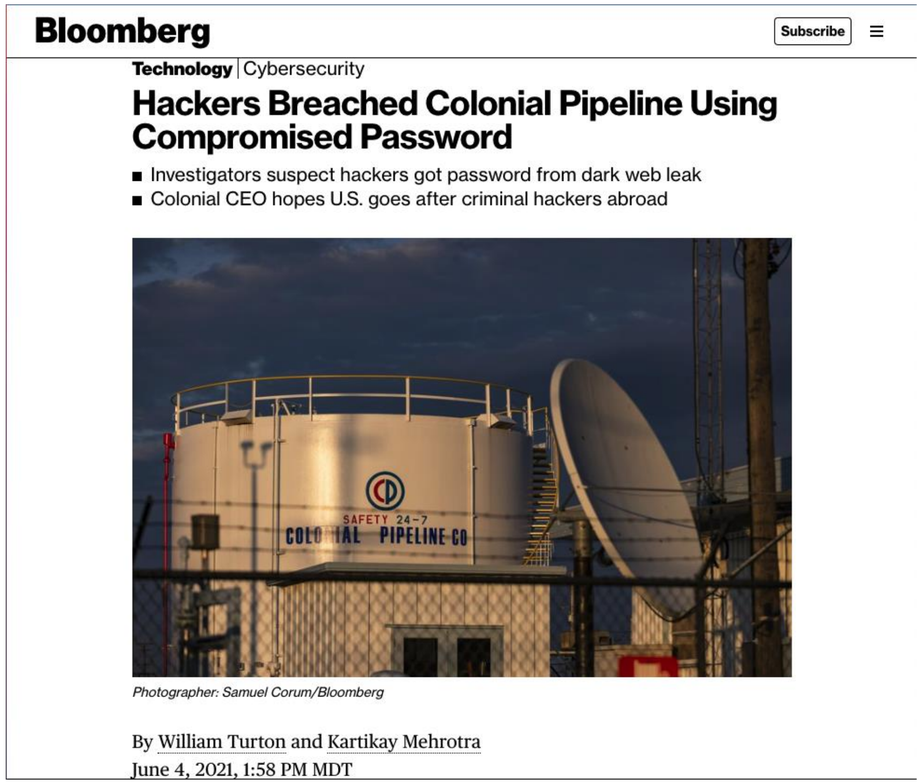
- Owners
- Designers
- Contractors
- Technology Partners



With Great Power Comes Great Responsibility

- Data Privacy Example – Cambridge Analytica + Facebook
- Cybersecurity Example – Colonial Pipeline Hack



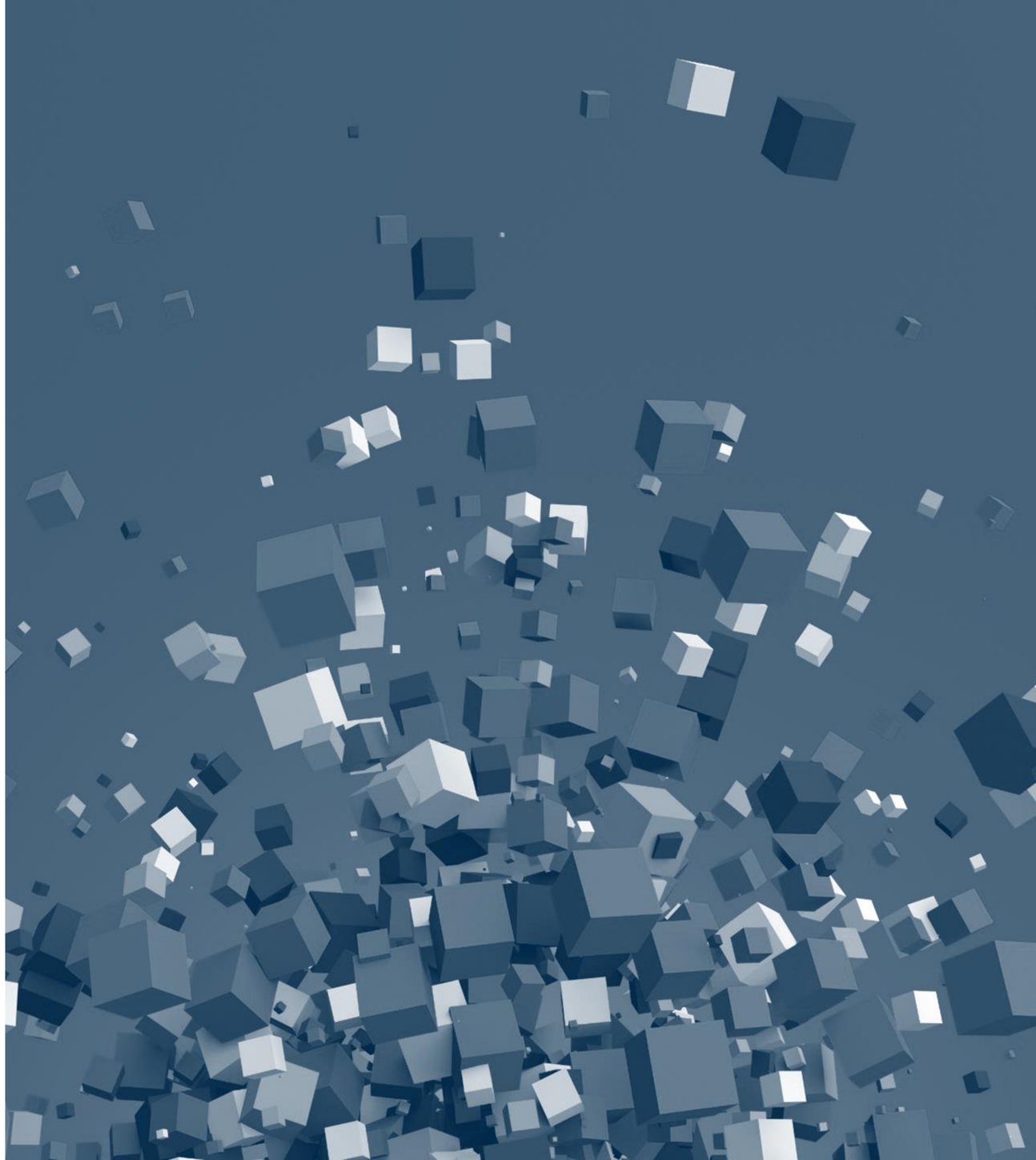


WHY ARE WE HERE?

PREPARE TO ENGAGE

Inspire broader understanding of the impacts of security and data privacy on collaborative digital delivery by doing the following:

1. Establish a shared vocabulary
2. Identify key impacts to the delivery process
3. Understand implications in technology, people and process
4. Compile real world feedback to Inform the U.S. National BIM Program's position on the matter



Areas of Impact

Why we should care?

The topics we will address in todays webinar are simply the beginning of what will be necessary to understand the impacts.

People

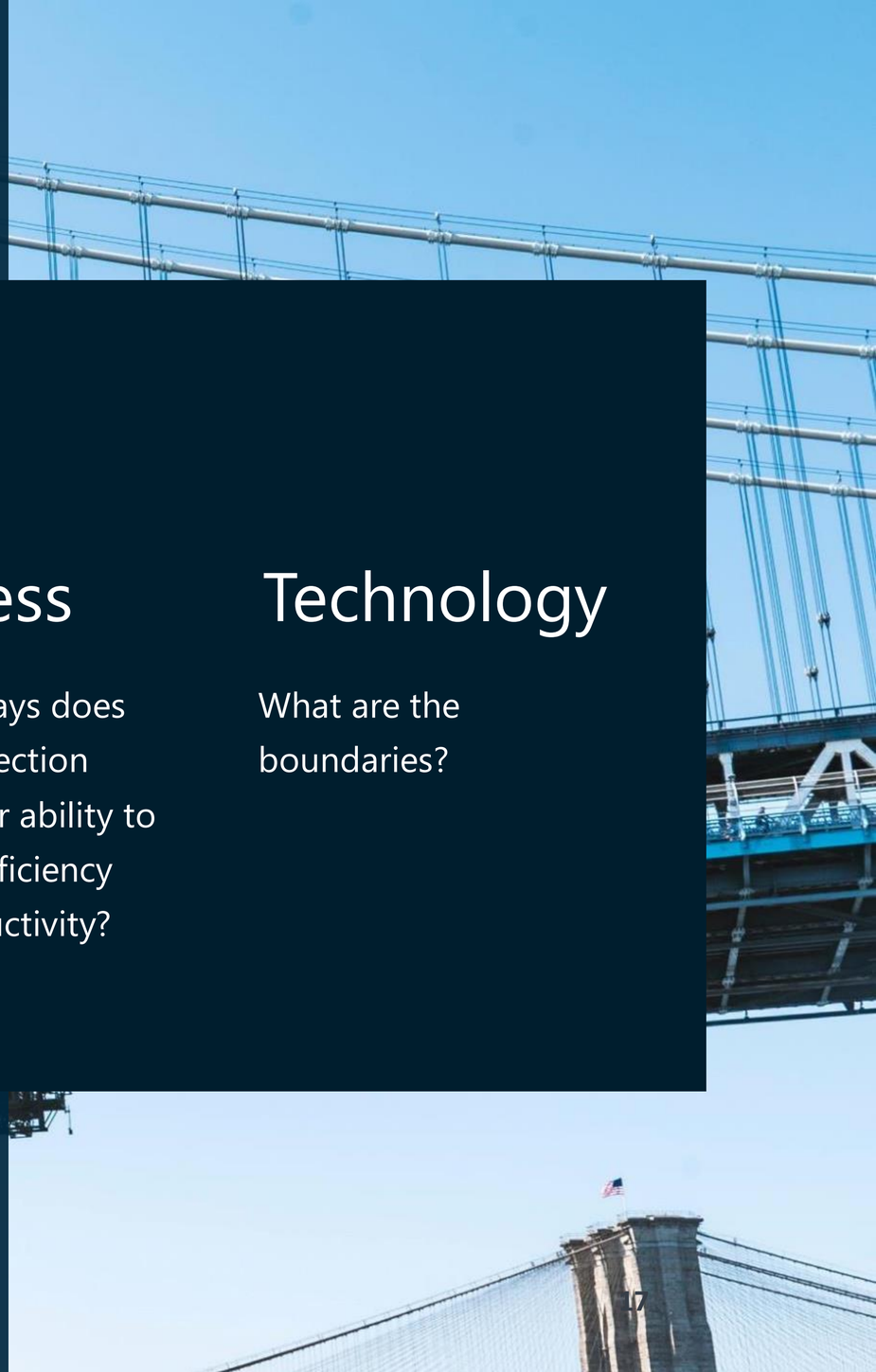
How does this impact our relationships and ability to achieve quality delivery?

Process

In what ways does this intersection impact our ability to achieve efficiency and productivity?

Technology

What are the boundaries?



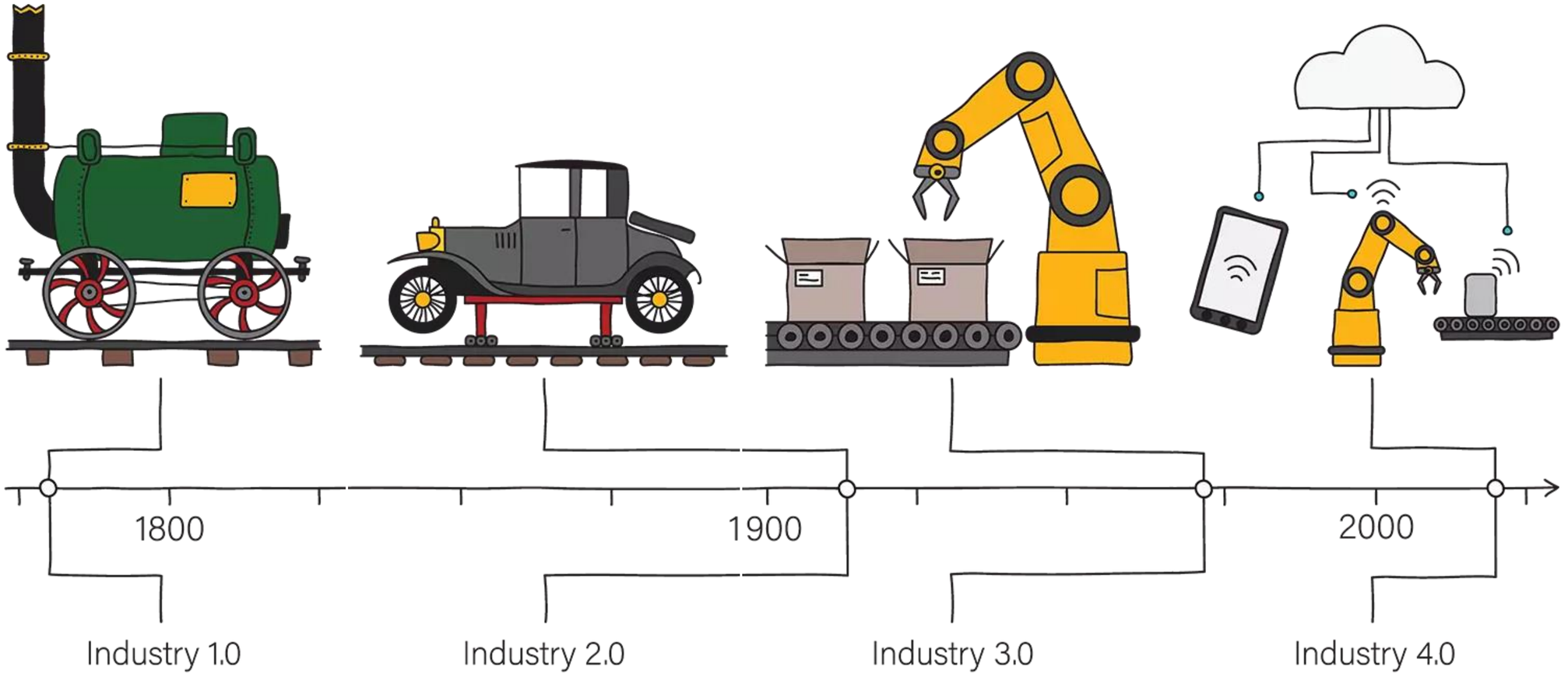
TECHNOLOGY

Industry 4.0 Impacts on AEC Collaboration

Nathan Wood

Executive Director | Construction Progress Coalition

Welcome to Industry 4.0



Industry 1.0

The Industrial Revolution begins. Mechanization of manufacturing with the introduction of steam and water power

Industry 2.0

Mass production assembly lines using electrical power

Industry 3.0

Automated production using electronics, programmable logic controllers (PLC), IT systems and robotics

Industry 4.0

The 'Smart Factory'. Autonomous decision making of cyber physical systems using machine learning and Big Data analysis. Interoperability through IoT and cloud technology.


The Economist
Crunch time in France
Ten years on: banking after the crisis
South Korea's unfinished revolution
Biology, but without the cells
MAY 6TH–12TH 2017
The world's most valuable resource
Data and the new rules of competition
Google
amazon
UBER
Microsoft
Google
TESLA
TESLA

Construction is Late to the Game.

McKinsey&Company

Imagining construction's digital future

Capital Projects and Infrastructure June 2016
McKinsey Productivity Sciences Center, Singapore

The construction industry is among the least digitized.

McKinsey Global Institute industry digitization index; 2015 or latest available data

Relatively low digitization — Relatively high digitization

● Digital leaders within relatively undigitized sectors

Sector	Assets			Usage					Labor			
	Overall digitization[1]	Digital spending	Digital asset stock	Transactions	Interactions	Business processes	Market making	Digital spending on workers	Digital deepening	Digital capital	Digitization of work
ICT[2]											
Media											
Professional services											
Finance and insurance											
Wholesale trade											
Advanced manufacturing											
Oil and gas											
Utilities											
Chemicals and pharmaceuticals											
Basic goods manufacturing											
Mining											
Real estate	●										
Transportation and warehousing	●										
Education	●										
Retail trade	●										
Entertainment and recreation											
Personal and local services											
Government	●										
Healthcare											
Hospitality	●										
Construction											
Agriculture and hunting											

[1]Based on a set of metrics to assess digitization of assets (8 metrics), usage (11 metrics), and labor (8 metrics).
[2]Information and communications technology.

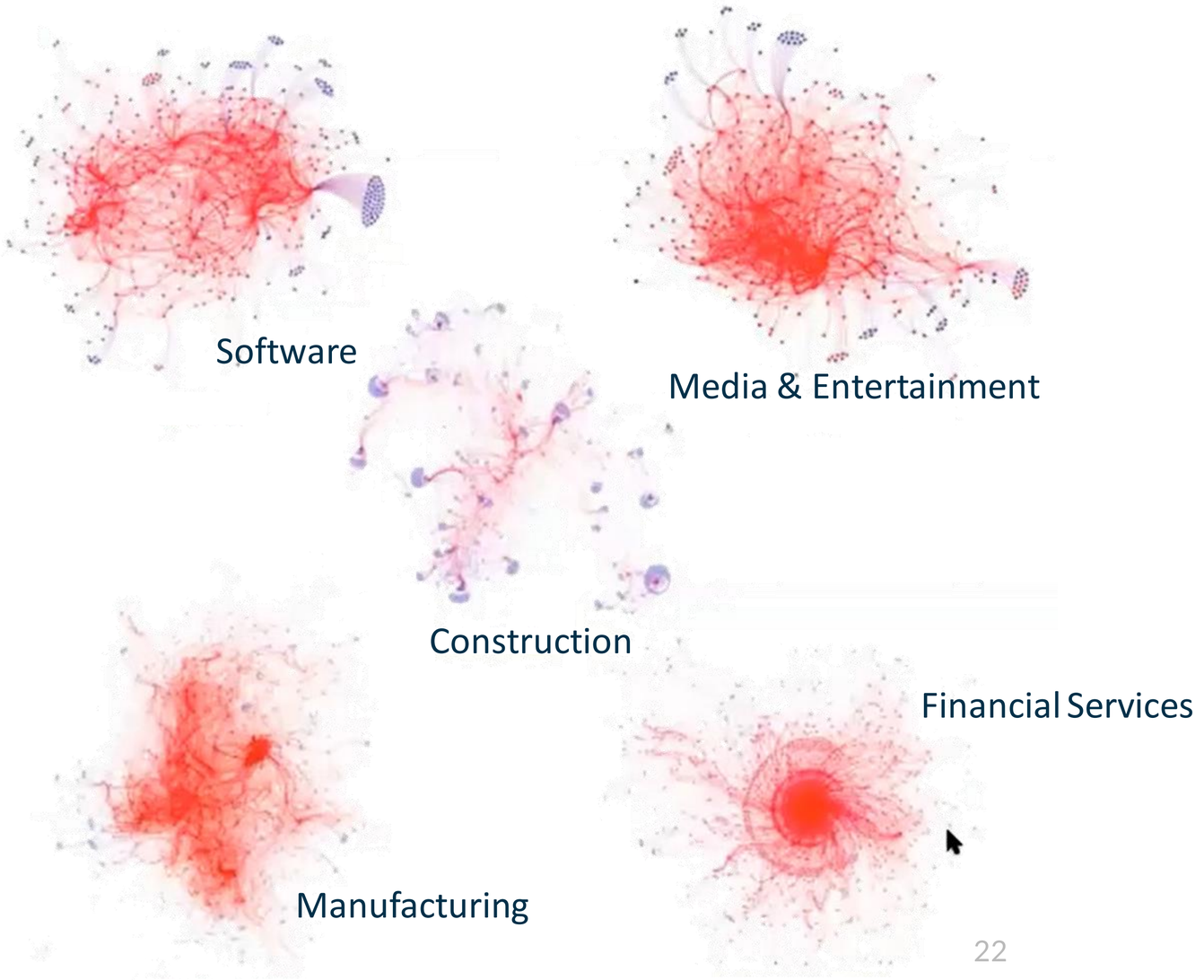
Source: AppBrain; Bluewolf; Computer Economics; eMarketer; Gartner; IDC Research; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; McKinsey Global Institute analysis

Visualizing Construction's #SharedPains

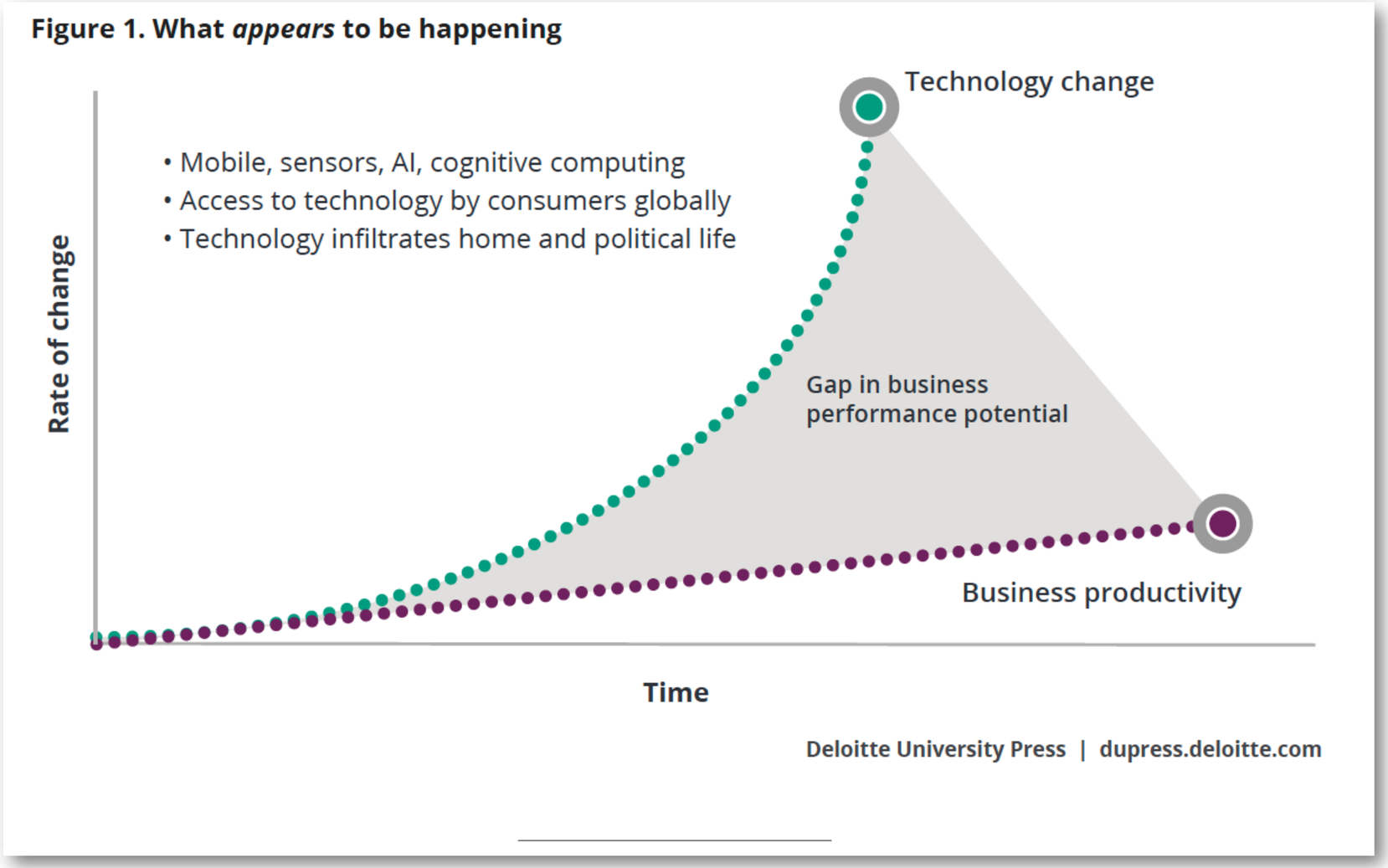
What does this say about our industry collaboration practices?

2014 Box.com File Exchange Metadata Analysis

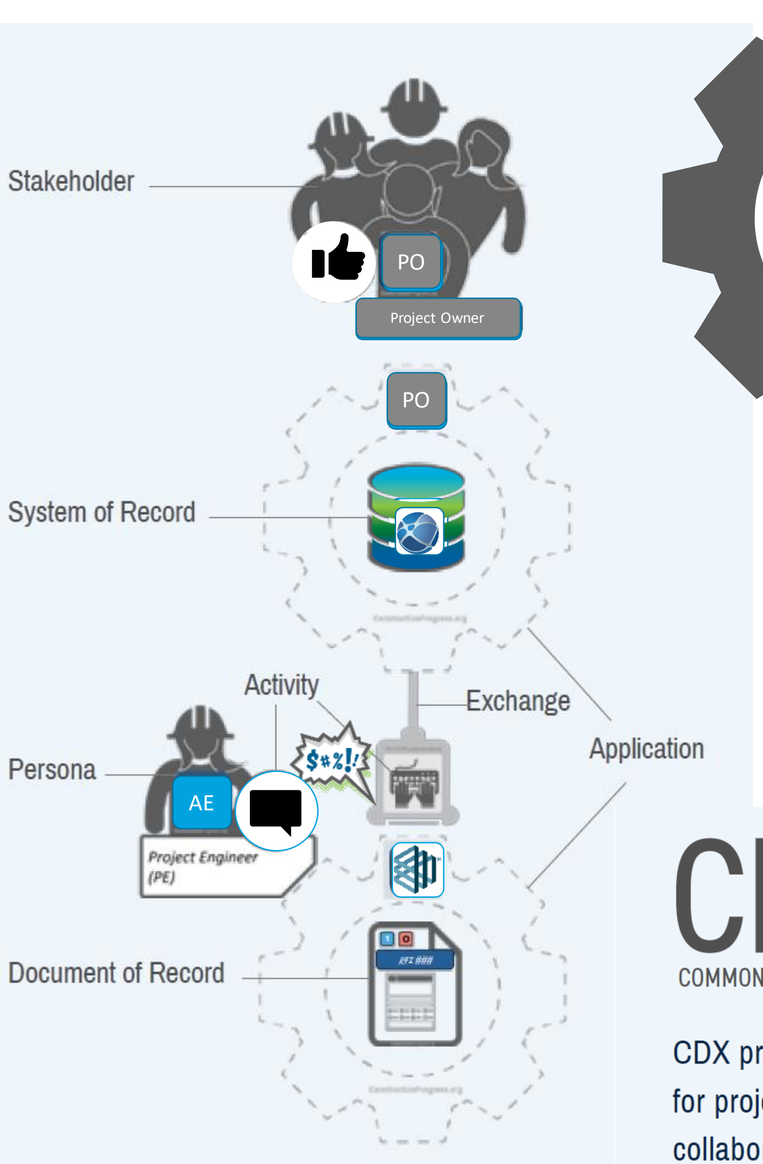
Red Node	Internal Company Data
Blue Node	External Collaborator Data
Red Edge	Connection from Internal
Blue Edge	Connection from External
Edge Width	Thicker edge represents more frequent connections between users

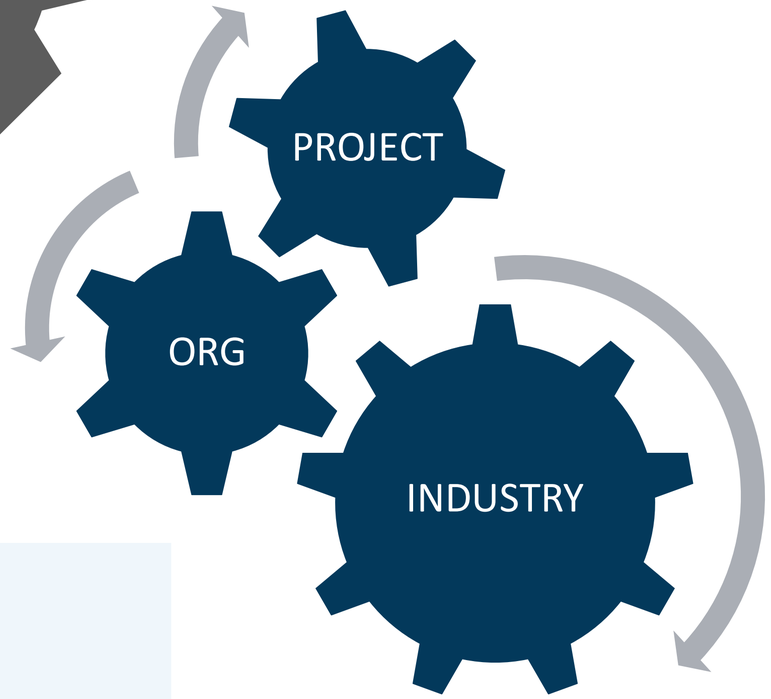


How is Industry 4.0 “Rewriting the rules” of design + construction?



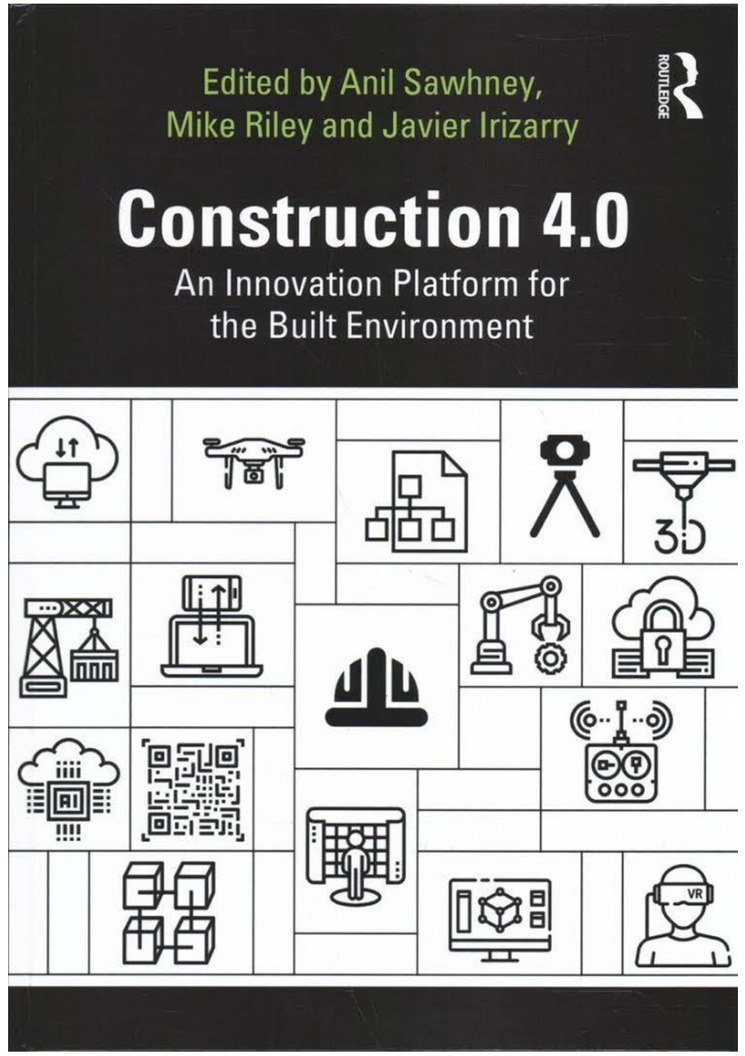
Do we have the tools we need for Construction 4.0?





CDX
COMMON **DATA** EXCHANGE

CDX provides a visual language for project teams to define their collaboration standards. Using:



TECHNOLOGY

Industry 4.0 Impacts on AEC Collaboration

Nathan Wood
Executive Director | Construction Progress Coalition

MENTIMETER: TECHNOLOGY

On your project, how many applications are used to share information or collaborate?

MENTIMETER: COOKIES

When prompted on a new website to accept cookies, what do you do??

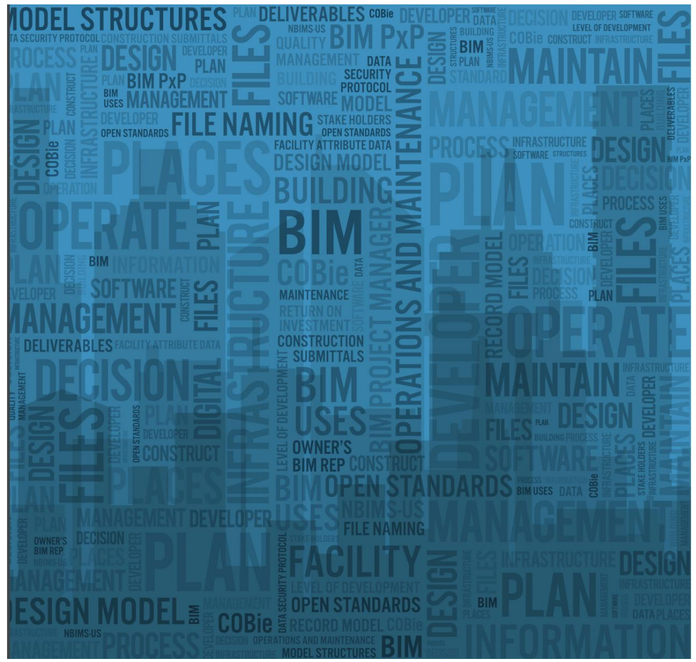
INFORMATION AND DATA PRIVACY

Foundational Legal Issues for Digital Delivery

Robert Prostko

Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer | Allegion

Foundational Legal Issues



Preliminary Intellectual Property, Privacy, and Cybersecurity Triage Questions

1. Who owns or has rights in the designs and data? Derivatives? Reuse?
2. Is personal data involved? If so, what privacy laws are applicable? Cross-border transfers?
3. What cybersecurity framework and controls, and/or laws apply? Is the project/information/data classified? Critical infrastructure? Covered by an NDA?

General Data Protection Regulation

- Data Subject Rights Requests
- Data Protection Impact Assessment
- Privacy-by-Design
  - 7 Foundational Principles by Ann Cavoukian, Ph.D.
    - Proactive not reactive; preventive not remedial
    - Privacy as the default setting
    - Privacy embedded into design
    - Full functionality – positive-sum, not zero-sum
    - End-to-end security – full lifecycle protection
    - Visibility and transparency – keep it open
    - Respect for user privacy – keep it user-centric
- Privacy-by-Default

U.S. State Privacy Laws and Effective Dates

State Privacy Law	Effective Date
California Consumer Privacy Act (CCPA)	**January 1, 2020**
California Consumer Privacy **Rights** Act (CPRA)	January 1, 2023
Colorado Privacy Act	July 1, 2023
Connecticut Data Privacy Act	July 1, 2023
Utah Consumer Privacy Act	December 31, 2023
Virginia Consumer Data Protection Act	January 1, 2023

Privacy News & Resources

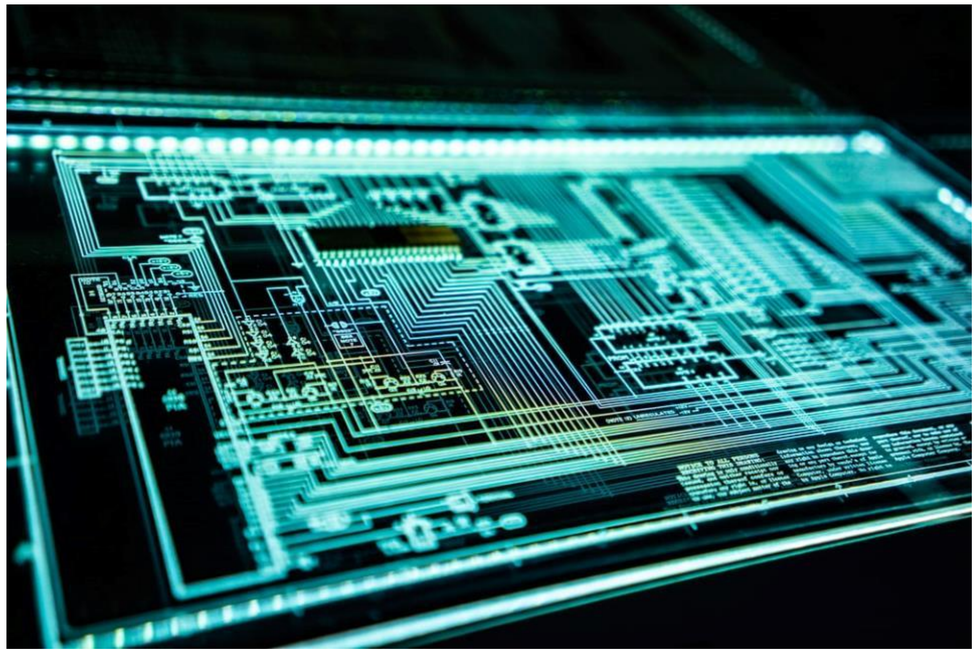
Inside Privacy Blog

International Association of Privacy Professionals (IAPP)

Common Privacy Themes Have Emerged

Notice	Legal Basis	Data Security	Breach Notice	Data Transfer
Proportionality	Minimization & Retention	Accountability	Data Subject Rights	Privacy-by-Design

Cybersecurity Standards and Laws



Depending on the nature and type of information and data, there are several different standards to align to or requirements that are applicable

NIST SP 800-171
(Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)

DFARS 252.204-7012
(Safeguarding Covered Defense Information and Cyber Incident Reporting)

FedRAMP
(Cloud authorization program for use with U.S. government)

ISO 27001
Information Security Management System

Secure, Scalable, and Simple

To be a great ecosystem partner, you need to master all three

Secure

Scalable

Simple

Physical ■ Digital ■ Cyber

INFORMATION AND DATA PRIVACY

Foundational Legal Issues for Digital Delivery

Robert Prostko

Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer | Allegion

MENTIMETER: COOKIES

When prompted on a new website to accept cookies, what do you do??

MENTIMETER:
IMPACT OF REQUIREMENTS

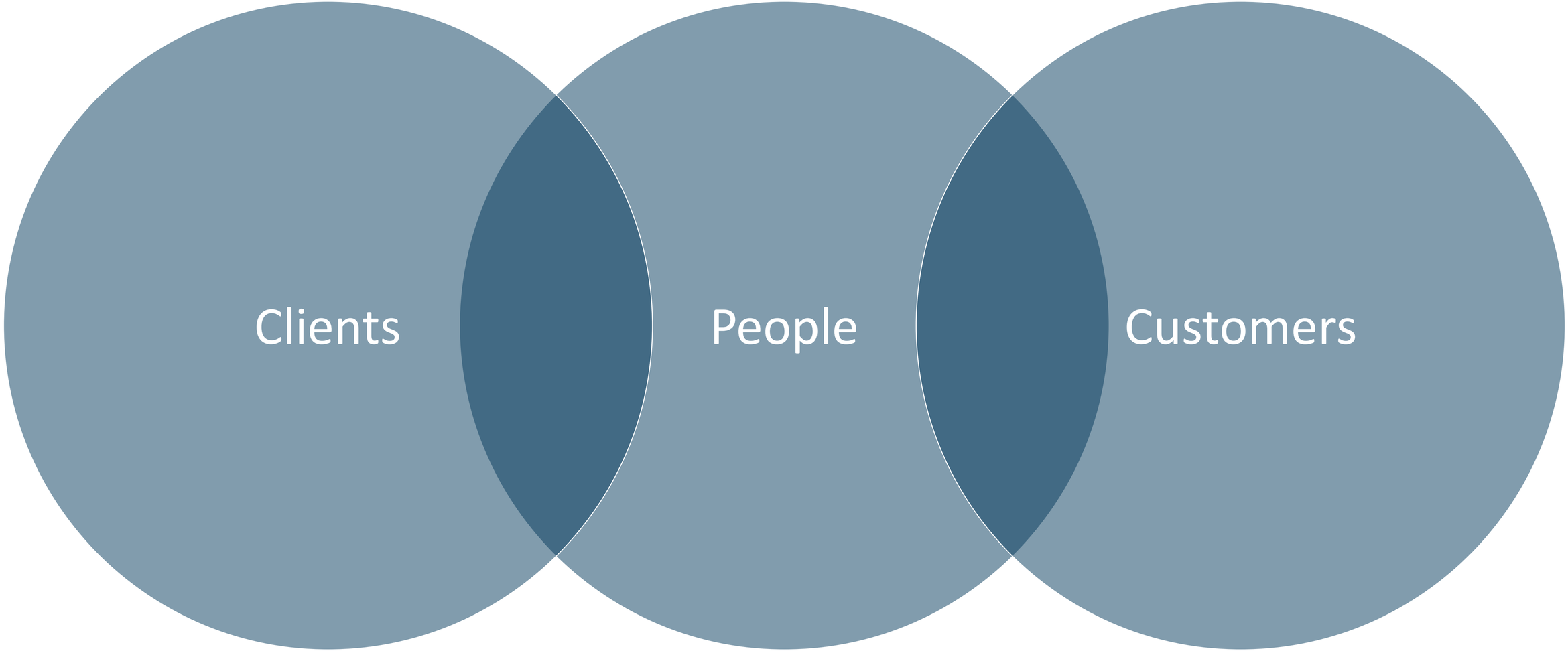
Rate the impact the following will have on your organization.

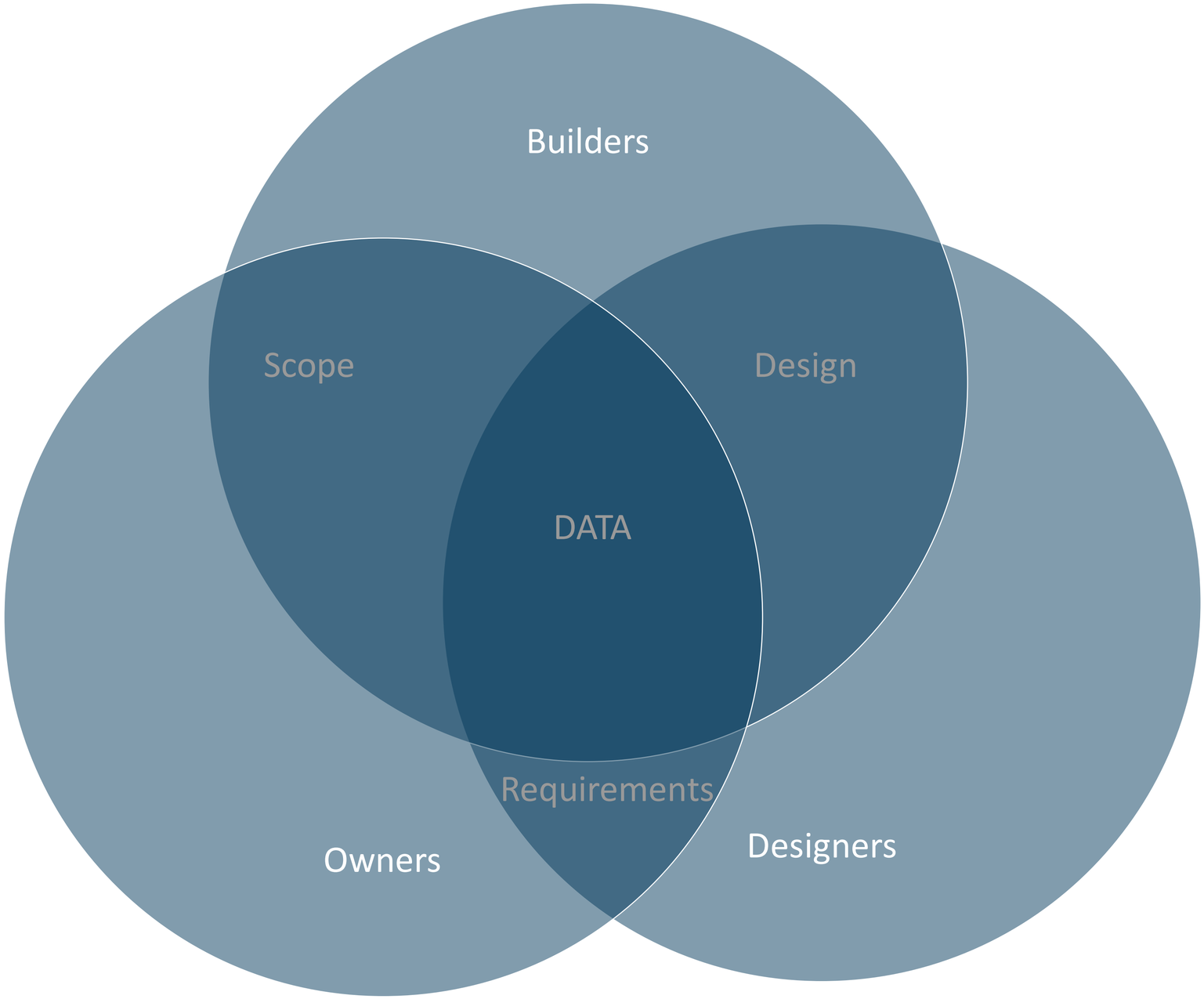
PEOPLE

Where perspective and motivation overlap

Brok Howard

Product Manager | dRofus


Clients
People
Customers


Builders
Scope
Design
DATA
Requirements
Owners
Designers

MENTIMETER:
IMPACT OF REQUIREMENTS

Rate the impact the following will have on your organization.

MENTIMETER: PERCEIVED RISK

What is the greatest risk to your organizations cybersecurity?

CUI TODAY

Working with Controlled Unclassified Information

Lynn Burns
ISSM & FSO | HDR Inc.

Controlled Unclassified Information (CUI)

The White House
Office of the Press Secretary

For Immediate Release — November 04, 2010

Executive Order 13556 -- Controlled Unclassified Information

All Unclassified Government Information Requiring Protection due to Law or Policy

US Critical Infrastructure Sectors where CUI may be a requirement


Chemical Sector


Energy Sector


Commercial Facilities Sector


Financial Services Sector


Food and Agriculture Sector


Communications Sector


Government Facilities Sector


Critical Manufacturing Sector


Healthcare and Public Health Sector


Information Technology Sector


Dams Sector


Nuclear Reactors, Materials, and Waste Sector


Defense Industrial Base Sector


Transportation Systems Sector


Emergency Services Sector


Water and Wastewater Systems Sector

Government CUI

Current Policies

Bureau of Reclamation SLE 02-01, 6 Mar 2015

Department of Treasury, Directive 80-08, 19 Oct 2017

Department of Commerce (DOC) OPBM-NP-18-001, 14 Aug 2019

Department of Defense (DOD) 5200.48, 6 March 2020

Environmental Protection Agency (EPA) CIO 2158.0, 8 Dec 2020

General Services Administration (GSA) 2103.2, 10 Apr 2021

US Geological Survey (USGS) 431.7, 21 May 2021

Nuclear Regulatory Commission (NRC) MD 12.6, 3 Dec 2021

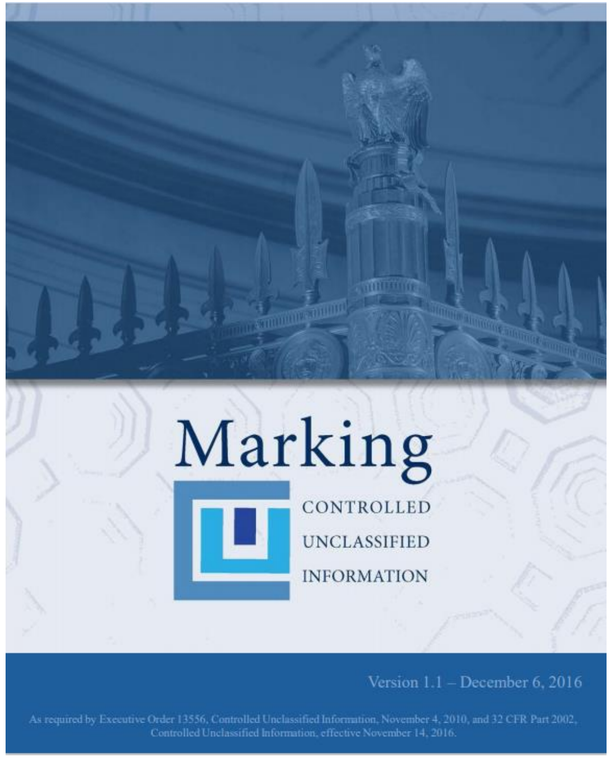
Tennessee Valley Authority (TVA) CUI Policy, 31 Dec 2021

Department of Energy (DOE) O 471.7, 3 Feb 2022

Department of Transportation (DOT) Order 1650.5, 10 Feb 2022

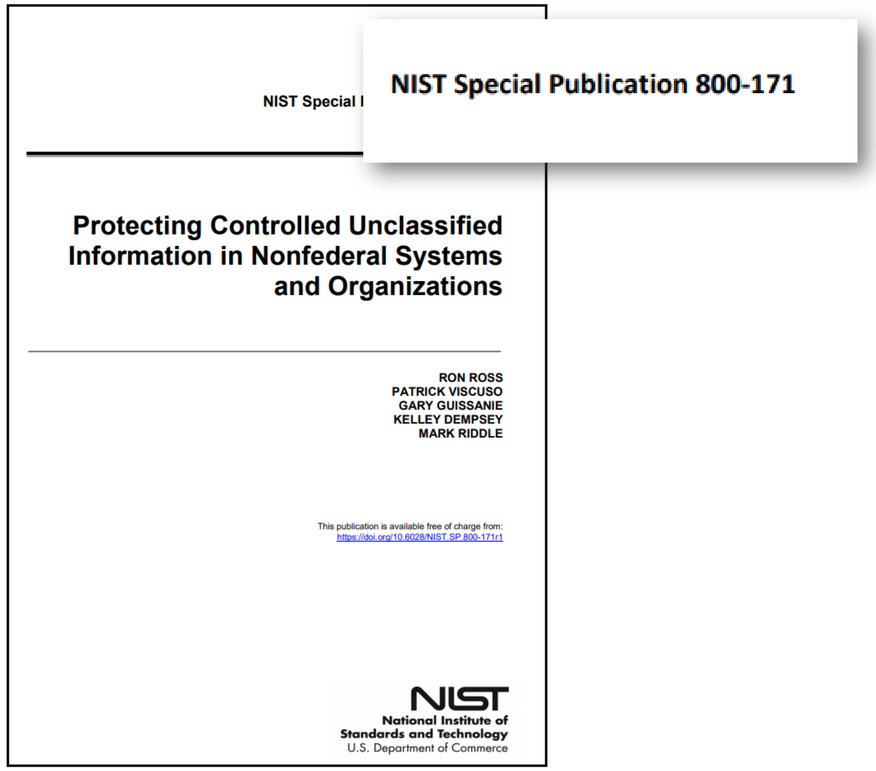
Federal Requirements for CUI in Industry's Hands

Physical Protections



Document Marking Requirements:
Banners, Paragraph Markings, Distribution Statements, Shipping Protection, Access Limitation, and Lockable Storage

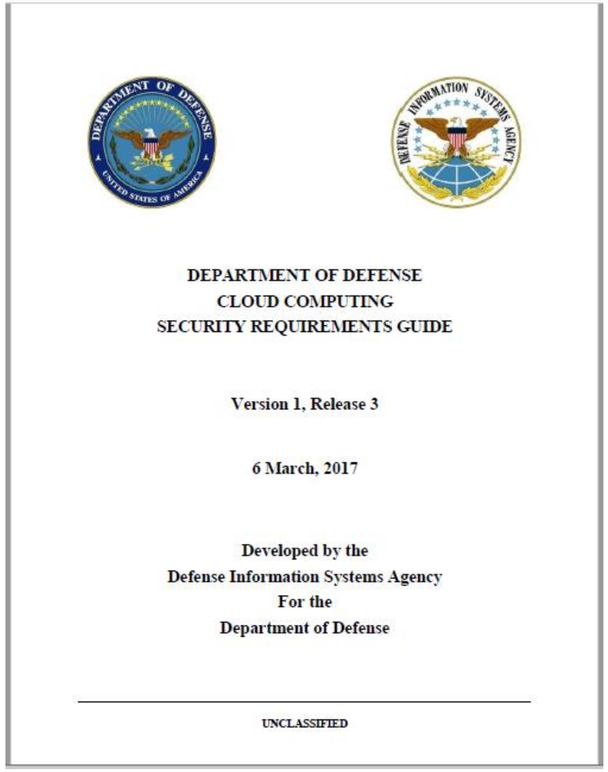
Digital Protections



110 Cyber requirements:
Policies, Procedures, Checklists, Inventories, Two-Factor Login, Encryption, Access Controls, and Audits

CUI in the Cloud - FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.



DOD Cloud Computing Security Requirements Guide
details protection requirements or DOD CUI protected by Cloud Service Providers

The Next Step:
Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) will become a requirement for performance on Federal contracts in 2023.

Certification will require **all companies** working with controlled unclassified information to **pass a NIST 800-171 audit** by an external organization.

Government contracting officers will verify certification prior to contract award.

Prime contractors may be denied an award if a subcontractor/teammate does not meet the CMMC requirements.

CUI TODAY

Working with Controlled Unclassified Information

Lynn Burns
ISSM & FSO | HDR Inc.

MENTIMETER: PERCEIVED RISK

What is the greatest risk to your organizations cybersecurity?

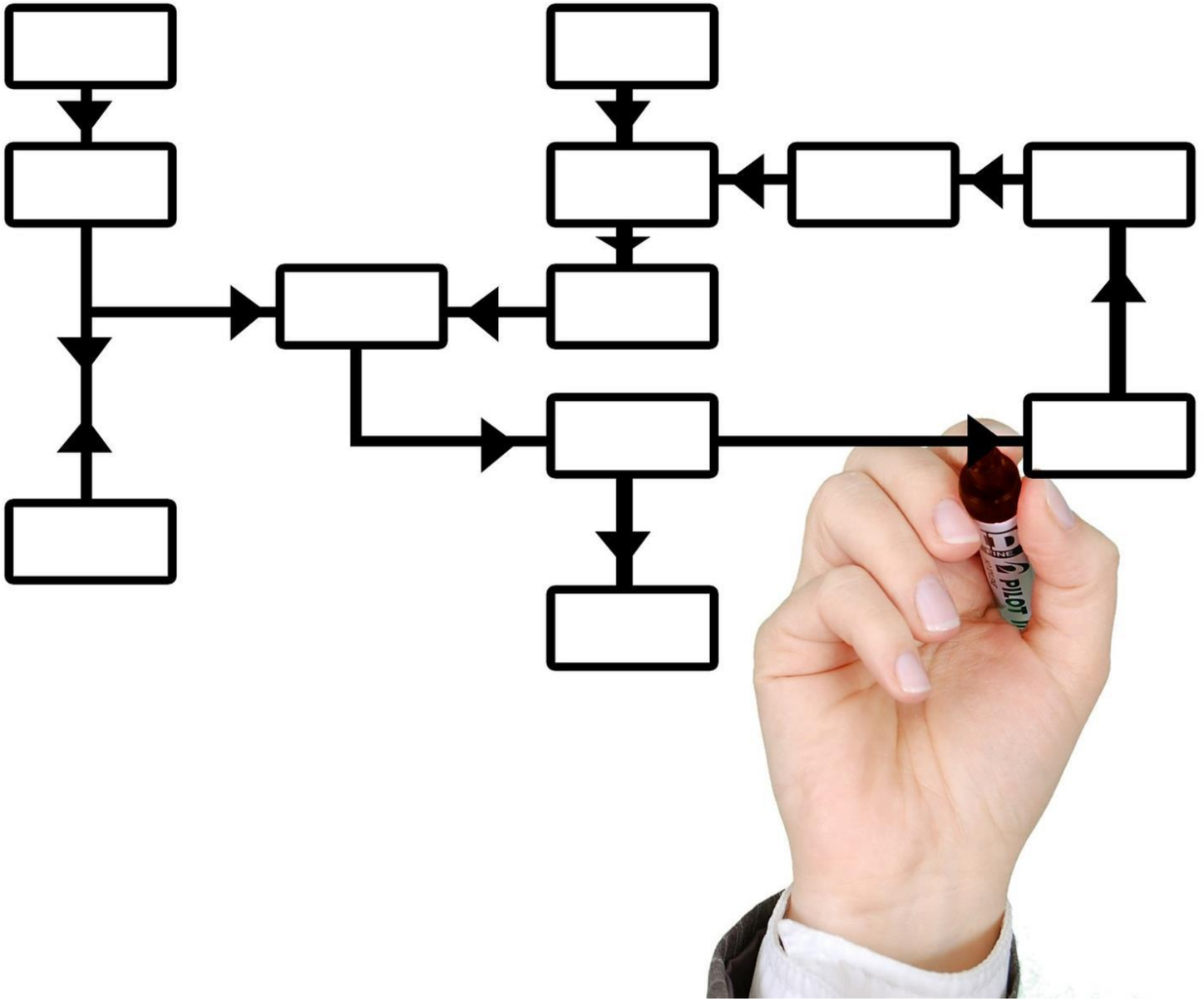
MENTIMETER: NIST 800-171

How relevant is the NIST 800-171/CMMC (110 security measures) to your current/future work?

PROCESS

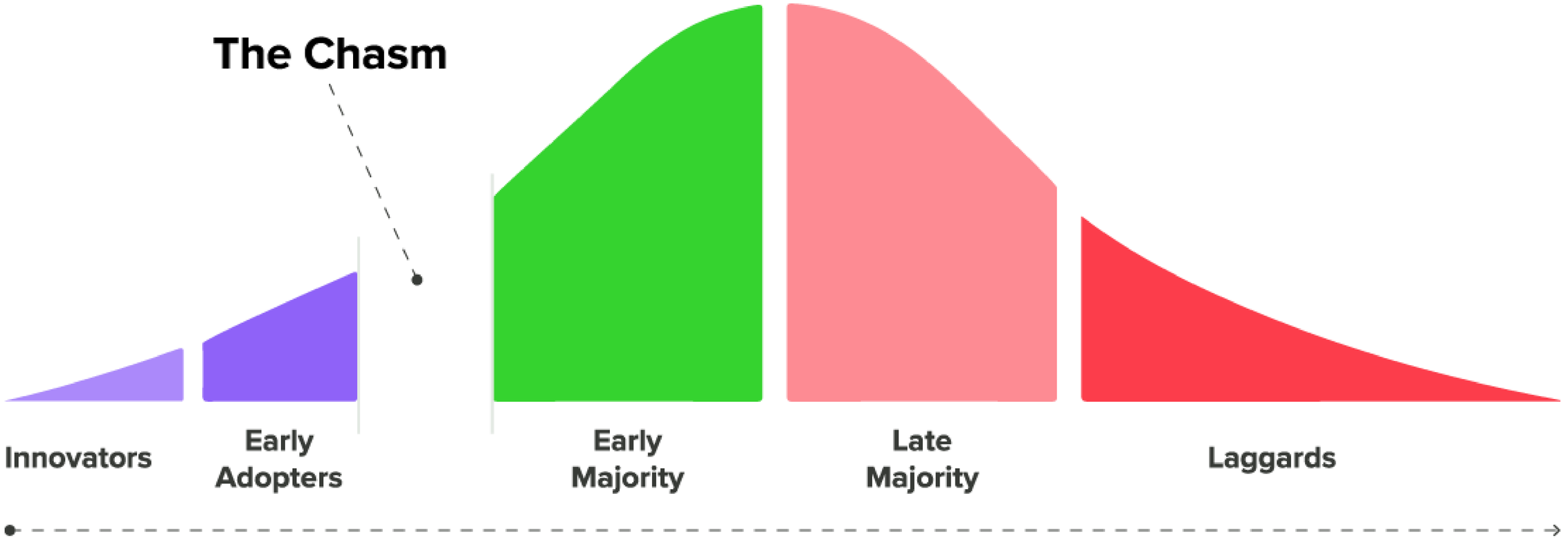
HOW DO NEW STANDARDS AFFECT OUR WORKFLOWS?

Connor Christian
Product Manager | Procore Technologies



What's inhibiting our move to new standards?

1. Tools need to be updated
2. Processes need to be updated
3. Stakeholders need to be trained


The Chasm
Innovators
Early Adopters
Early Majority
Late Majority
Laggards

MENTIMETER: NIST 800-171

How relevant is the NIST 800-171/CMMC (110 security measures) to your current/future work?

MENTIMETER:
IMPACT ON DELIVERY

How likely are the following to negatively impact your ability to deliver digitally?

FEDRAMP & THE AEC

What is FedRAMP and why do we need it?

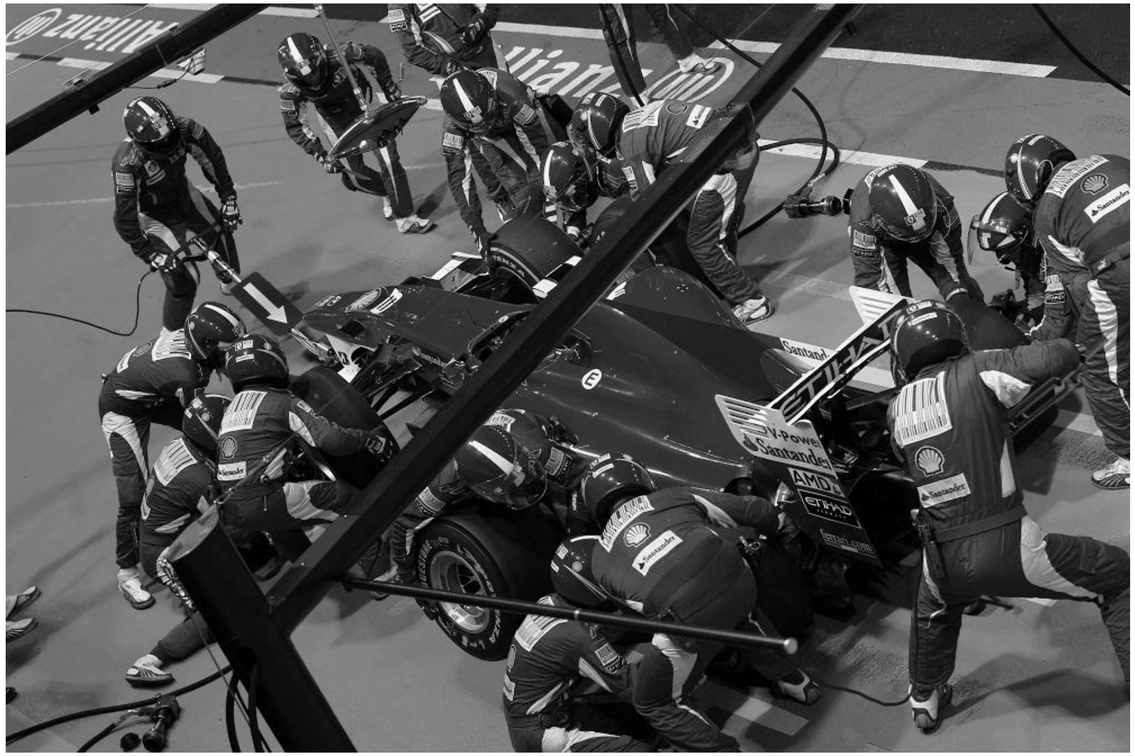
Horatio McDowney
IT Applications Project Specialist | U.S. General Services Administration

When You Are In a Race

- Early Years (First F1 1950)
- Dangerous
  - Refueling - banned in 2009
  - Pit lane directly adjacent to the track (cars moving at 180 mph)
- Limited Involvement
  - Two Mechanics
  - Now team of ~ 20 people
- Rough Tools
  - Using hammers to remove wheels
  - Today pneumatic wrenches (wheel guns)
- Long
  - Up to 60 seconds
  - Today ~ 2.5 seconds (3+ seconds slow)

Formula 1 Pit Stop

Photo: United Autosport via CC



AEC Would Like to Speed Up the Federal Security Process

FedRAMP designed to ensure security for cloud services for the federal government

- Long Process
  - 12-24 Month Long Process (2011-2015)
  - Now 6 to 12 Months
- Dangerous
  - Security of Cloud
  - More Dangerous Now
- Limited Involvement
  - White House and NIST Standards
  - Agency Involvement
- Rough Tools
  - 15 to 20 Security Documents
  - Li-SaaS and Mi-SaaS Processes

Formula 1 Pit Stop

Photo: United Autosport via CC

What is FedRAMP?

FedRAMP

FedRAMP is the Federal Risk and Authorization Management Program

- Cost-effective, risk-based approach for the adoption and use of **cloud services** by the federal government
- Emphasis on **security** and **protection** of federal information
- Reduces **duplicative** efforts, **inconsistencies**, and cost inefficiencies

FISMA

Federal Information Security Modernization Act (FISMA) requires agencies to protect federal information

OMB Circular A-130

Office of Management and Budget (OMB) states that when agencies implement FISMA, they must use National Institute of Standards and Technology (NIST) standards and guidelines

FedRAMP Policy

FedRAMP leverages National Institute of Standards and Technology (NIST) standards and guidelines to provide standardized security requirements for cloud services; a conformity assessment program; standardized authorization packages and contract language; and a repository for authorization packages

Who Is Involved in FedRAMP?

- **FedRAMP Program Management Office (PMO)**
  - The Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP. The JAB consists of the Chief Information Officers from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA)

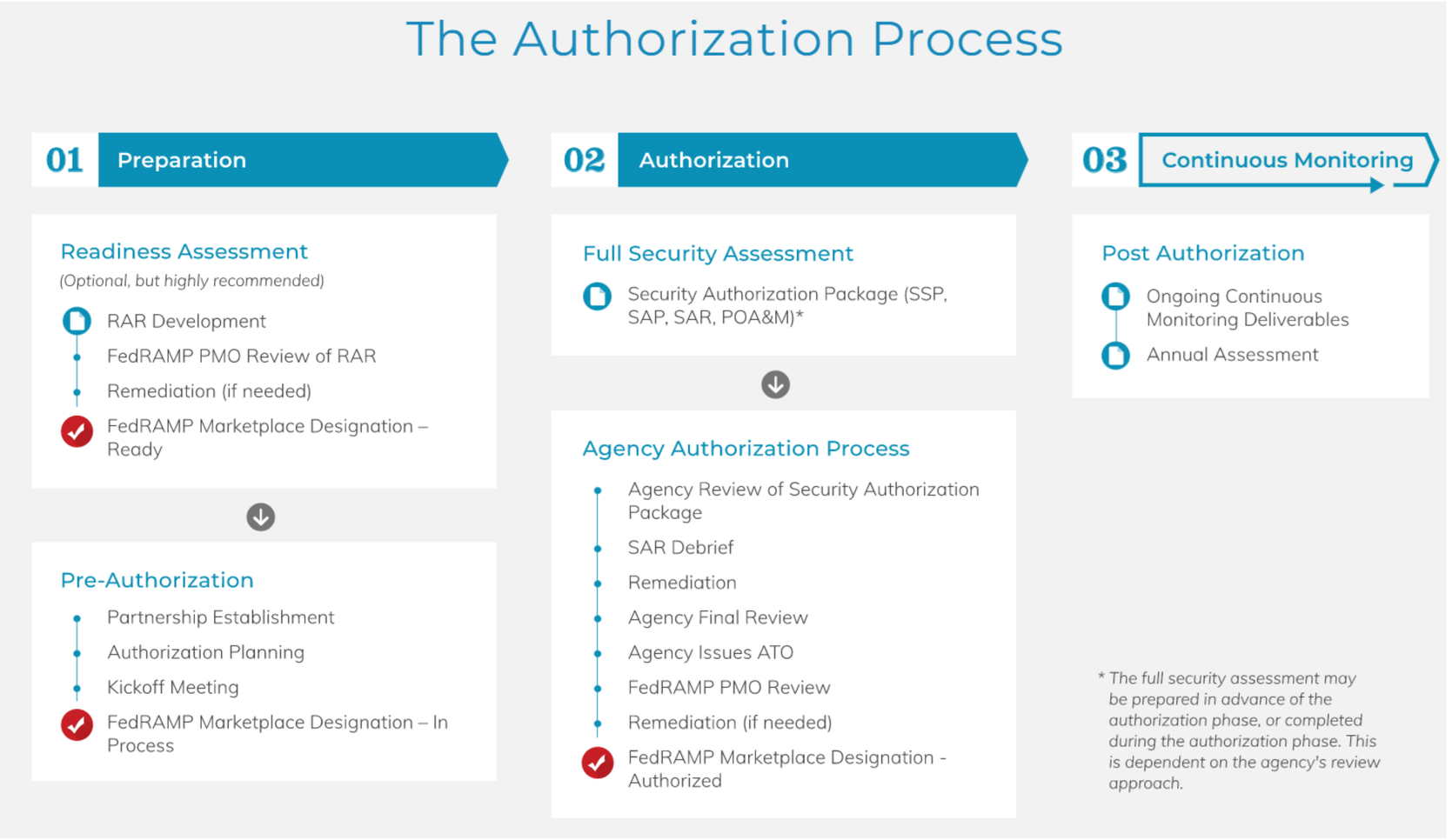
- **Cloud Service Providers (CSPs; vendors)**
  - CSPs only need to go through the FedRAMP Authorization process once for each Cloud Service Offering (CSO) and perform continuous monitoring

- **Third Party Assessment Organizations (3PAO)**
  - As independent third parties, they perform initial and periodic assessments of cloud systems based on federal security requirements
  - List on FedRAMP Marketplace

- **Agencies**
  - Agencies use FedRAMP's standardized baselines to evaluate the security of cloud services.
  - Work with CSPs to review the security posture and authorize the CSO

What Is the Wait?

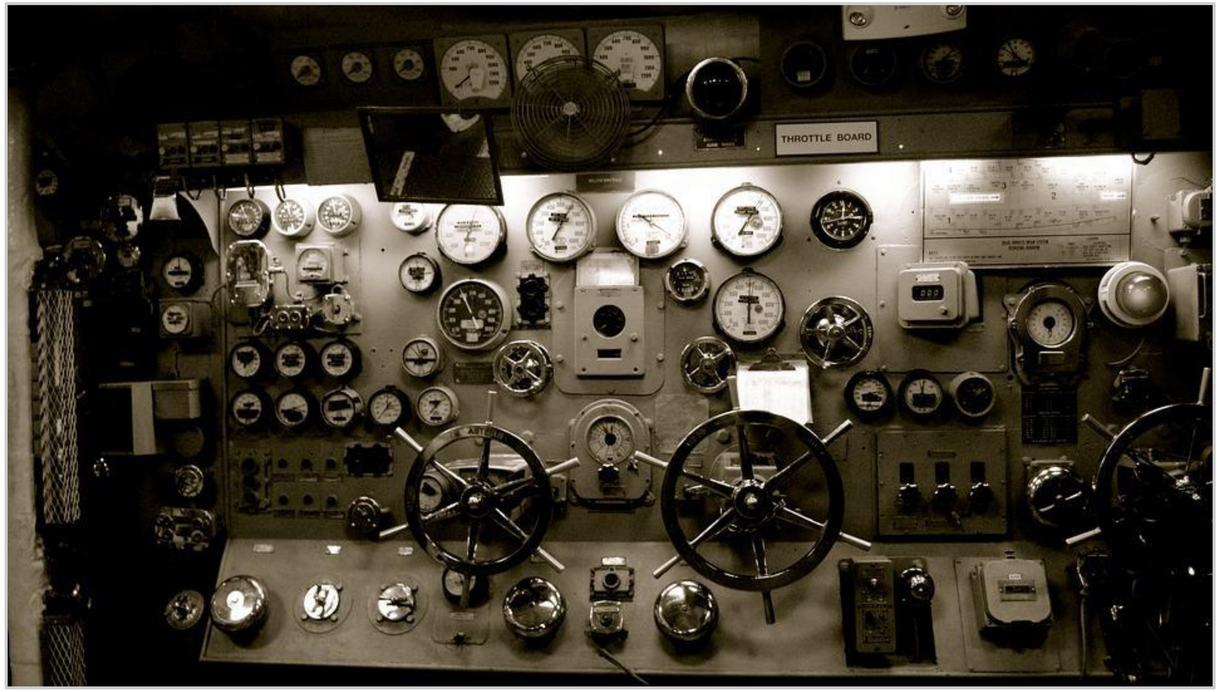
- Depends on Agency Buy-In
- Depends on Vendor
- Depends on Level



The Core: NIST Security Controls

Controls span the following: access, auditing (logs), pen testing, config, recovery/backup, authentication, incident response, maintenance, media, physical security, personnel security, sys communication, vulnerability scanning, code, boundary protection/keys

- **Li-SaaS - 37+ Controls**
  - Mostly attest and few document
- **Tailored (Low) Level - 125 Controls**
  - Attest and Document
- **Mi-SaaS (GSA Only) - 69+ Controls**
  - Mostly attest and more document
- **Moderate Level - 325 Controls**
  - Mostly Document and some attest
- **High Level - 421 Controls**
  - Document and some attest



What Is Produced Via the FedRAMP Process

- Completed about 35 Security Documents
- Authorization to Operate Issued
- Plan for Continued Monitoring Including
    - Reviews of all documentation
        - Inclusion of additional components or capabilities
    - Remediation of any findings
    - Tasks for agency to ensure secure usage
    - Tasks for renewal/reissuance of ATO

What You Can Do to Prepare

- **Educate Yourself and the CSP**
  - What is the CSO and what parts will be targeted for the initial ATO?
  - Get them a list of the controls to evaluate their application
  - If they don't have a 3PAO make sure they know they need one
- **Get IT Involved Early**
  - If your IT team can't understand it, your security team may struggle
- **Get Security Involved Early**
  - Requesting FedRAMP Package
- **Answer Questions (with Your IT and Security Team)**
  - Help teams understand what application does
    - Get solid description of the application from IT
  - How will access be granted into system? Volume of users? Environments?
  - What systems will be integrated? How? What types of data? (field level)
  - What types of users?
  - Who will be managing the application?

Watch Out for Common Dangers in the Pit

- **False Starts**
  - Other security accreditations (StateRAMP)
- **Stalling**
  - Not having the right people
  - Not having the FedRAMP Package
  - Not understanding what CSO (or parts of the CSO) are targeted for an already accredited offering
    - Always ask: “Is that feature FedRAMP approved?”
- **Needing a Tune Up**
  - CSP attempting to circumvent controls
- **Fires**
  - CSP targeting wrong Impact Level

Formula 1 Pit Stop

Photo: United Autosport via CC

Additional Resources

- **FedRAMP Resources**
  - FedRAMP Website
    - Templates for Process
    - Training
      - Subscribe
    - Baselines
- **NIST Resources**
  - Control Resources
    - Families
- **GSA Resources**
  - IT Security Resources (procedural guidance on authorization process for each security level)

NIST Website (Families)
Explanation of Controls

SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

Control Families

AC - ACCESS CONTROL
AT - AWARENESS AND TRAINING
AU - AUDIT AND ACCOUNTABILITY
CA - ASSESSMENT, AUTHORIZATION, AND MONITORING
CM - CONFIGURATION MANAGEMENT
CP - CONTINGENCY PLANNING
IA - IDENTIFICATION AND AUTHENTICATION
IR - INCIDENT RESPONSE
MA - MAINTENANCE
MP - MEDIA PROTECTION
PE - PHYSICAL AND ENVIRONMENTAL PROTECTION
PL - PLANNING
PM - PROGRAM MANAGEMENT
PS - PERSONNEL SECURITY
PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
RA - RISK ASSESSMENT
SA - SYSTEM AND SERVICES ACQUISITION
SC - SYSTEM AND COMMUNICATIONS PROTECTION
SI - SYSTEM AND INFORMATION INTEGRITY
SR - SUPPLY CHAIN RISK MANAGEMENT

Jump To:

REVISION 5.1

Home
Control Families
Low-Impact
Moderate-Impact
High-Impact
Privacy Control Baseline
All Controls
Search

FEDRAMP & THE AEC

What is FedRAMP and why do we need it?

Horatio McDowney

IT Applications Project Specialist | U.S. General Services Administration

MENTIMETER:
IMPACT ON DELIVERY

How likely are the following to negatively impact your ability to deliver digitally?

MENTIMETER: ISO

What is your familiarity with ISO 19650?

ISO 19650 – PART 5

A security minded approach to information management

Rahul Shah
Sector Director | BSI Group Inc

WHAT IS ISO 19650?

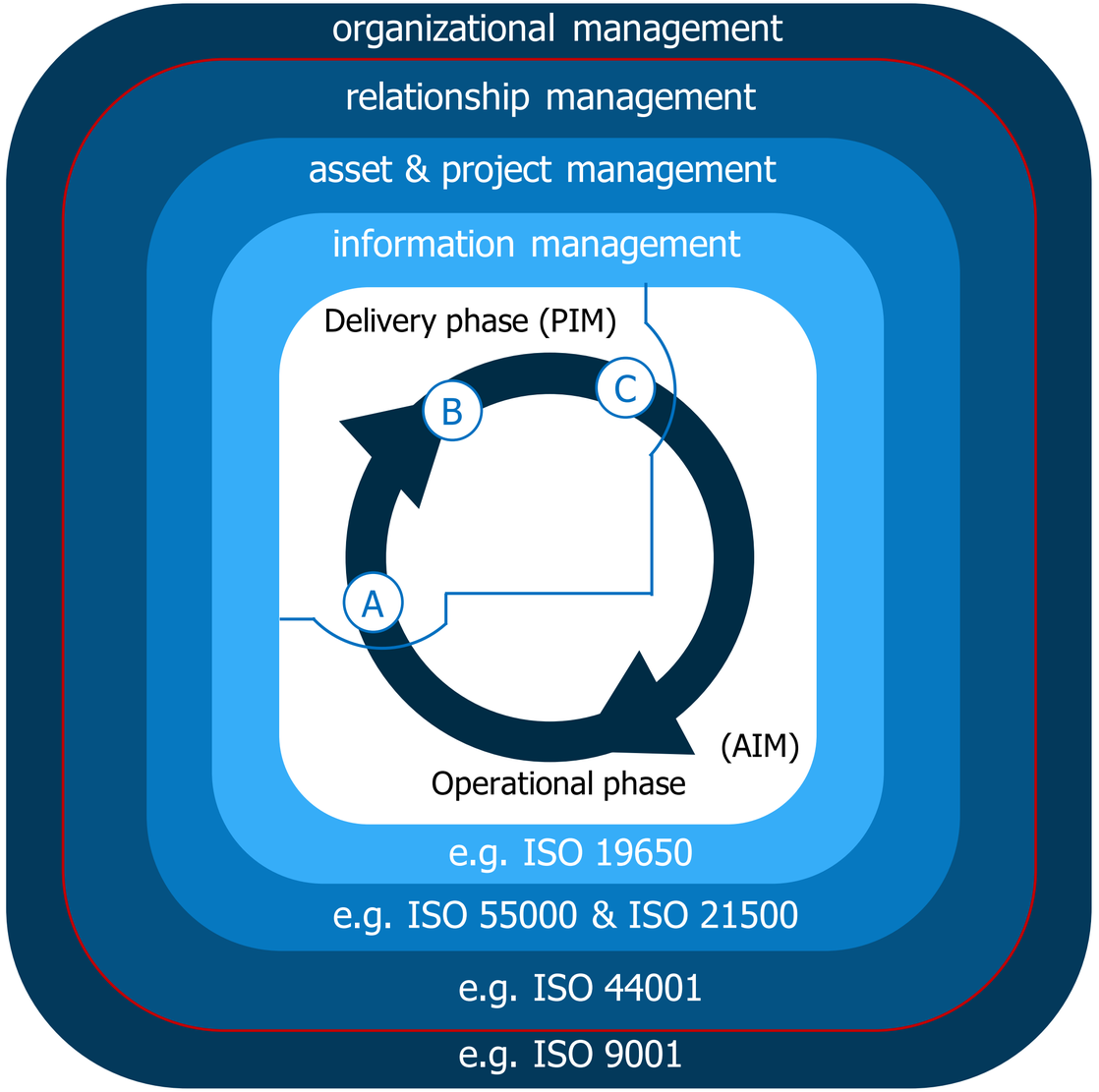
Published as an international standard in 2018 based on BS 1192 and PAS 1192, this standard supports the organization and digitization of information about buildings and civil engineering works through building information modelling (BIM)

1 Information management

a Organization of information

b Digitization of information

INFORMATION MANAGMEENT – IN THE CONTEXT OF ORGANIZATIONAL MANAGEMENT



ISO/IEC 27001
Information Security

[SOURCE: ISO 19650 , modified]

“SECURITY MINDED” PROJECT INFORMATION MANAGEMENT

ISO 19650 is separated into multiple (soon to be six) parts. Each impacts a range of stakeholders at different times in the asset lifecycle.

applies to all stakeholders in design, construction, & operations

ISO 19650-1
Concepts & Principles

ISO 19650-5
Security-minded Approach

applies to designers, general contractors, trade contractors

ISO 19650-2
Delivery Phase

applies to asset owners and operators

ISO 19650-3
Operational Phase

[ISO 19650-4]
(to be published in 2022)
Information Exchange

[ISO 19650-6]
(TBD)
Health & safety

Security-minded

Understanding and routinely applying **appropriate and proportionate measures** [to achieve a] state of **relative freedom from potential cause** of an incident which may result in **harm in any business situation** so as to deter and/or disrupt deliberate, unwanted, hostile, malicious, fraudulent and criminal behaviours or activities

COMPARISON: ISO 27001 (ORG) TO ISO 19650 PART 5 (PROJECT)

ISO 27001

Information security management

Information security requirements for an **individual** organization

ISO 27001 demonstrates your commitment to managing information safely and securely **for all operations in your organization**

ISO 19650 Part 5

Security-minded approach to information management (BIM)

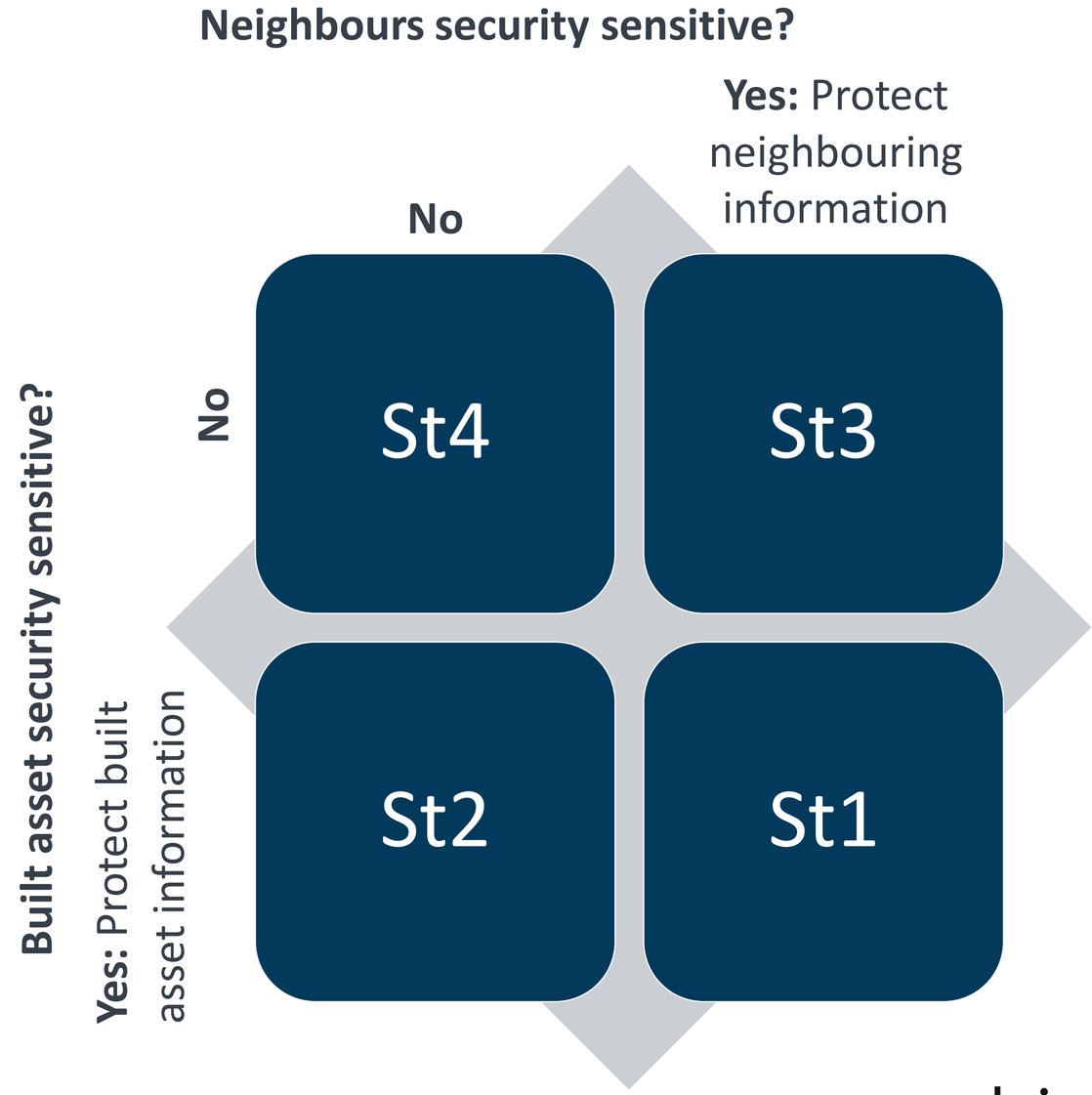
The adoption of security-minded, risk-based approach that can be applied across, as well as within **multiple** organizations

ISO 19650 part 5 demonstrates your adoption of a proportional security-minded information management **using BIM throughout the lifecycle of an asset**, where sensitive information is obtained, created, processed, and/or stored

IMPLEMENTING ISO 19650 PART 5 – SECURITY STRATEGY

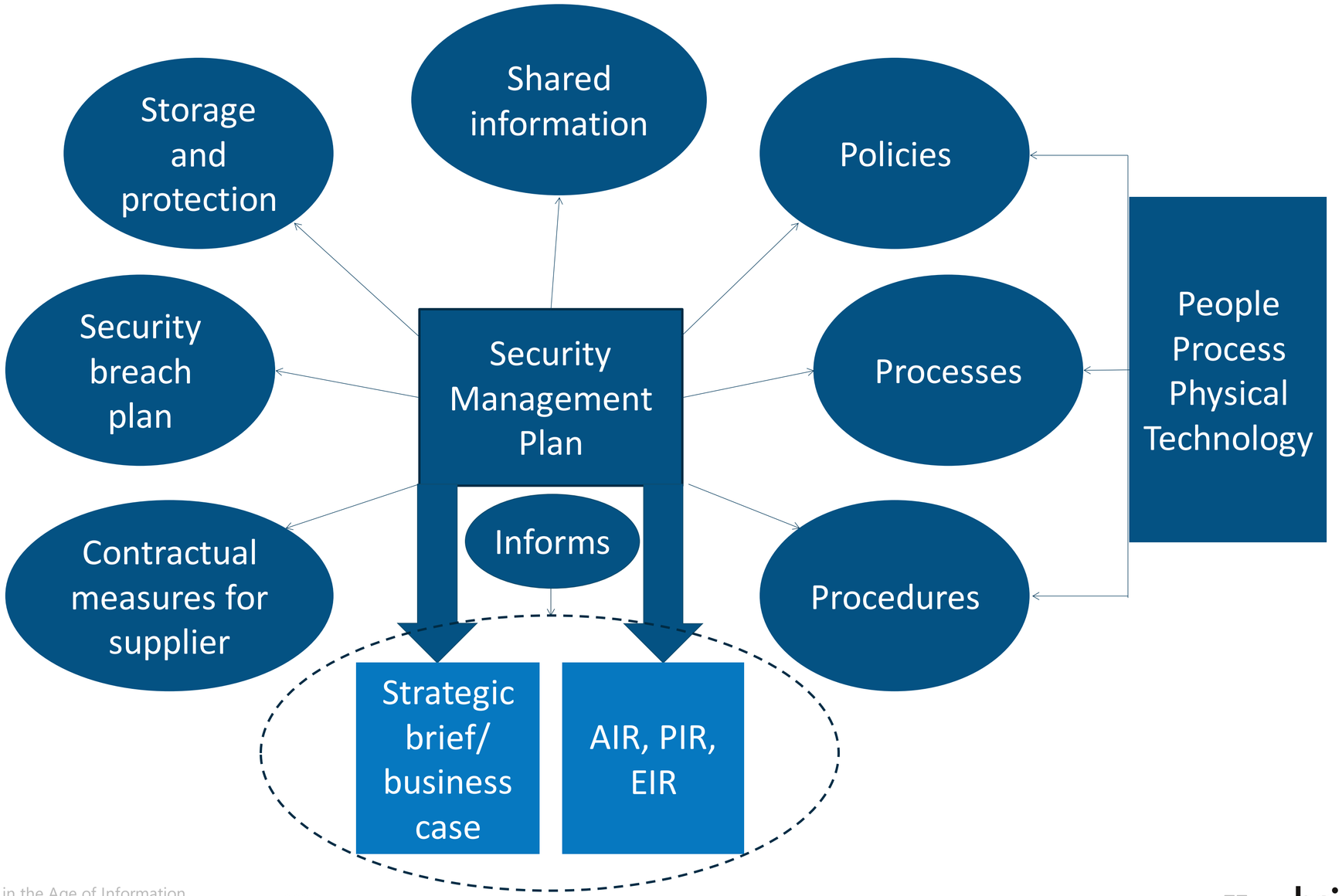
(Ultimate accountability has to remain with the asset owner or project client)

Establishing governance, accountability and responsibility for the security-minded approach. The top management shall appoint an individual at top management level accountable for the security-minded approach.



IMPLEMENTING ISO 19650 PART 5 – SECURITY MANAGEMENT PLAN

- Ultimate accountability has to remain with the asset owner or project client.
- Enables the agreed mitigation measures set out in the security strategy to be implemented in a consistent and holistic manner.



ISO 19650 – PART 5

A security minded approach to information management

Rahul Shah
Sector Director | BSI Group Inc

MENTIMETER: ISO

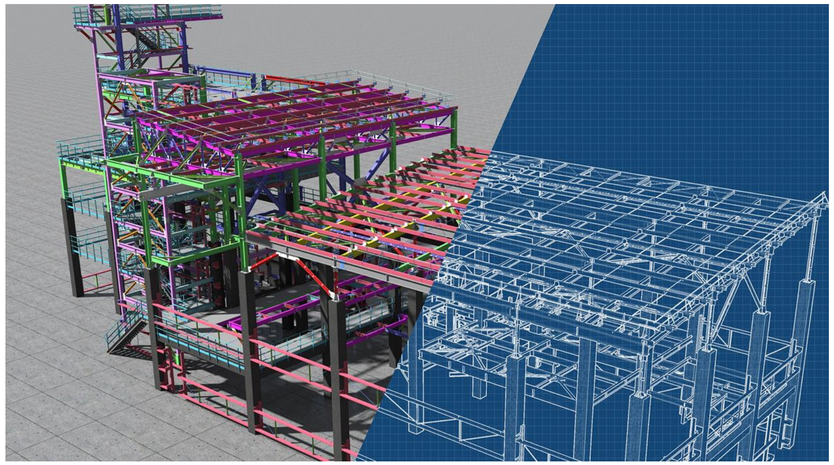
What is your familiarity with ISO 19650?

NATIONAL STANDARDS

Requirements in practice: An international perspective

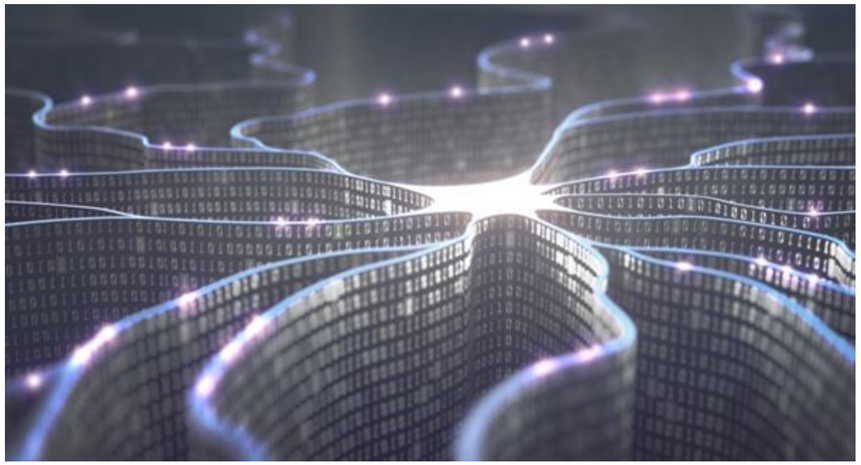
Alexandria Luck
Fellow | The Institution of Civil Engineers

WHAT HAS CHANGED?



Increased use, and reliance on digital and communication technologies

Increased collaborative working



Greater sharing of information (open data)

WHAT IS THE THREAT?







SECURITY GOVERNANCE

- Top management
- Accountability
- Responsibility

WHAT IS SENSITIVE?

Developing and maintaining a holistic approach

Information security

- Personnel security
- Physical Security
- Cyber Security

Your organization

Your supply chain

NATIONAL STANDARDS

Requirements in practice: An international perspective

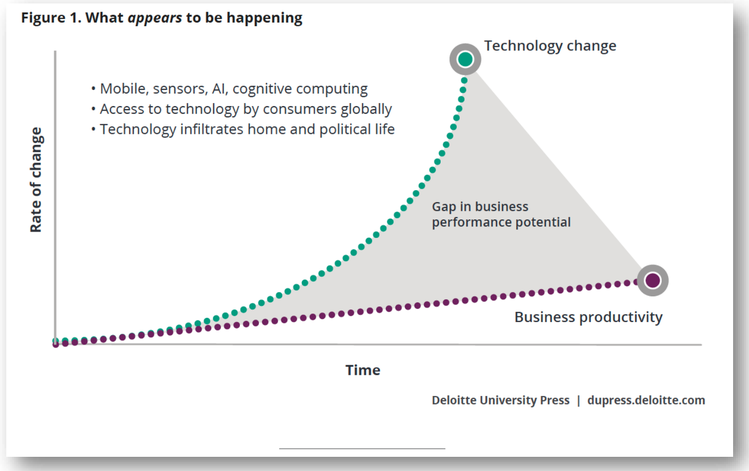
Alexandria Luck
Fellow | The Institution of Civil Engineers

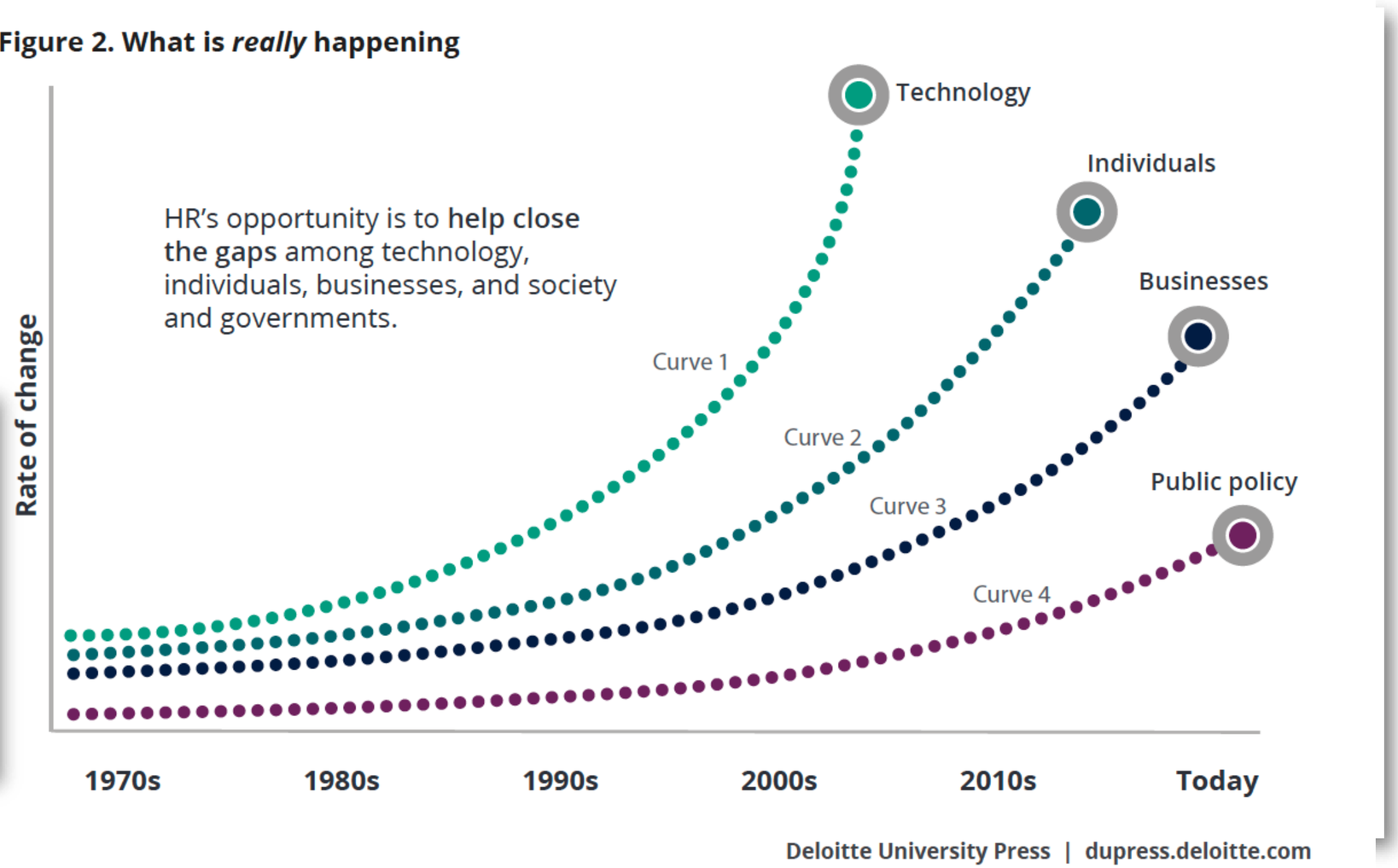
MENTIMETER: SECURITY APPROACH

How does your organization approach security?

Digital Transformation….It's Complicated.

In Reality, Digital Transformation Requires Multiple Parties to Align





WHAT'S NEXT?

To move forward together the conversation must continue.
Here are the next steps for the National BIM Program:

Collaborative Digital Delivery and Security Workshop

National BIM Program leadership convenes

Building Innovation (September 2022)

THANK YOU!

Share your feedback in the follow up survey.