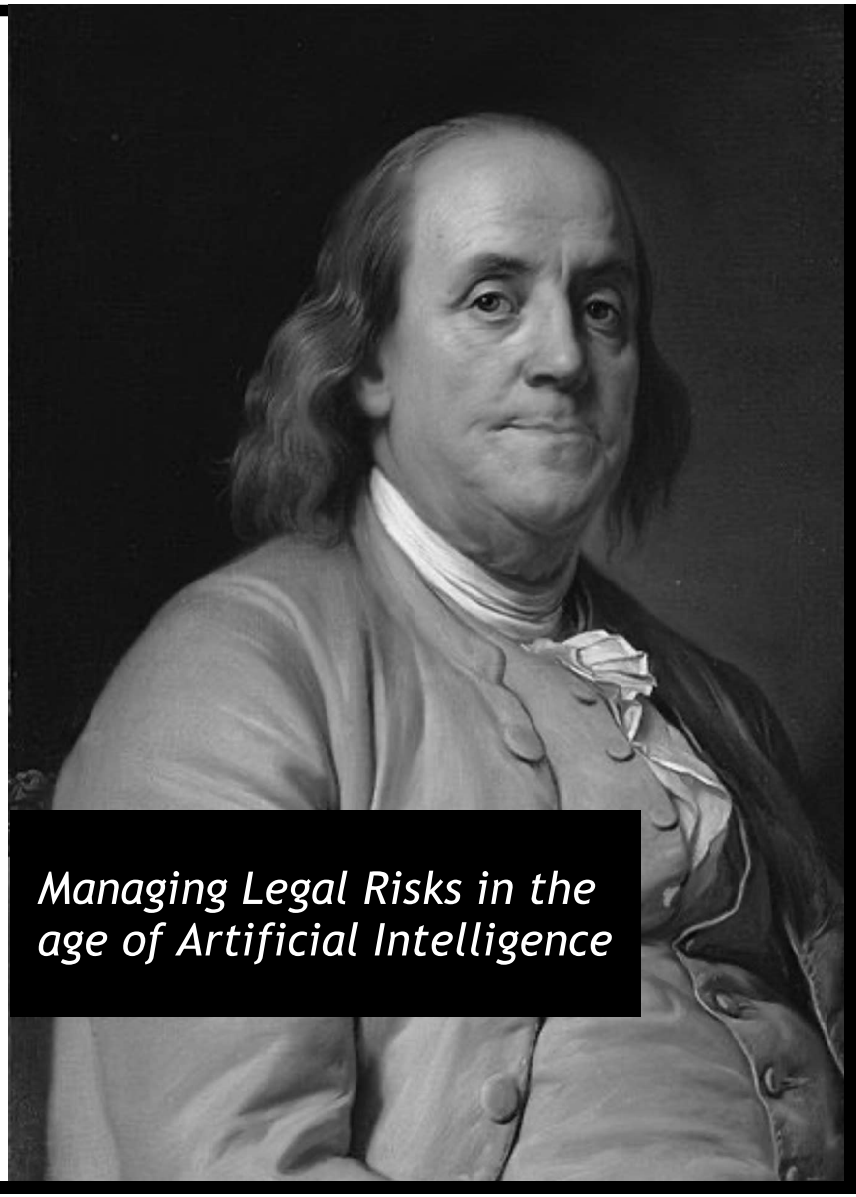
HEART OF AMERICA
TAX INSTITUTE
Nov. 7 2024

CYBER SECURITY

DATA STORAGE & INFORMATION PRIVACY

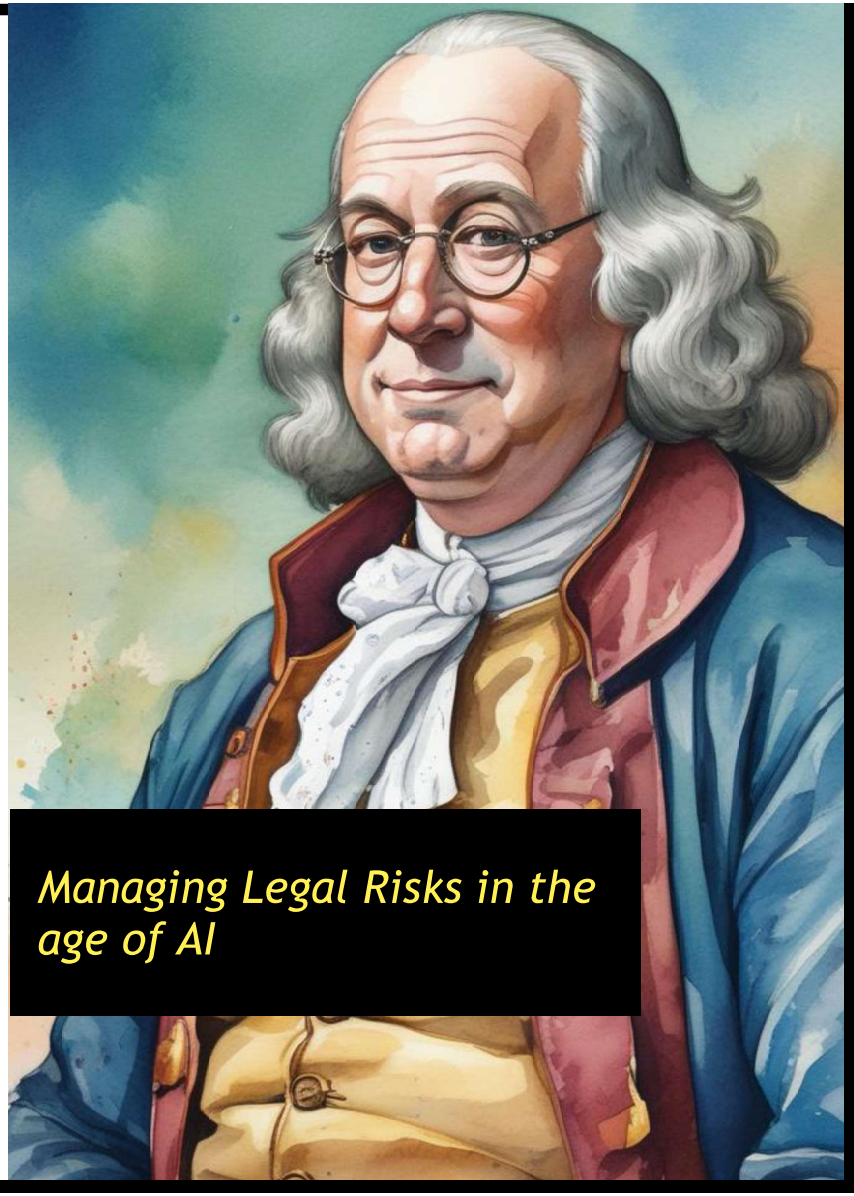


Managing Legal Risks in the age of Artificial Intelligence

HEART OF AMERICA
TAX INSTITUTE
Nov. 7 2024

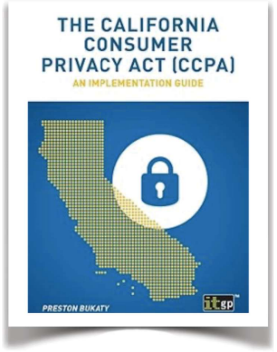
CYBER SECURITY

DATA STORAGE & INFORMATION PRIVACY



INTRODUCTION

- Preston Bukaty, Denver, CO
  - *Sr. Compliance Attorney, IntelePeer*
  - Juris Doctorate, Univ. of Kansas School of Law
- Author, "The CCPA: An Implementation Guide"
- prior: *GRC Consultant, IT Governance USA*
  - Advise clients on data privacy and cybersecurity laws
  - Training & certification courses covering evolving laws (GDPR, CCPA), and respective risk management frameworks (ISO 27001, NIST 800-53)
- Questions? Email questions to pbukaty@sbcglobal.net



AGENDA

1. Data, breaches, and the importance of information
2. AI laws & compliance requirements
3. Where to start? The cybersecurity lifecycle
4. The cybersecurity lifecycle - Preparation
5. The cybersecurity lifecycle - Detection & analysis
6. The cybersecurity lifecycle - Respond

3 Important Statistics About How Much Data Is Created Every Day

FinancesOnline
REVIEWS FOR BUSINESS

1 How much data is generated every minute?

Source: Domo

41,666,667
messages shared by WhatsApp users

1,388,889
video / voice calls made by people worldwide

404,444
hours of video streamed by Netflix users

347,222
stories posted by Instagram users

150,000
messages shared by Facebook users

147,000
photos shared by Facebook users

2 Estimated Data Consumption from 2021 to 2024

Source: IDC / Statista

3 Data Growth in 2021

Sources: TechJury, Internet Live Stats, Cisco, PurpleSec

2 TRILLION
searches on Google by the end of 2021

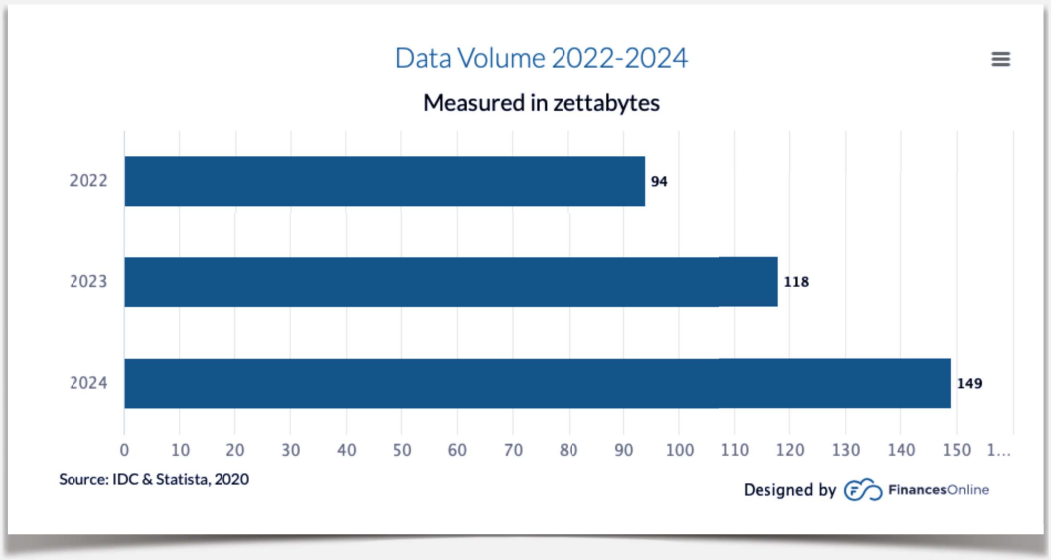
1.134 TRILLION MB
volume of data created every day

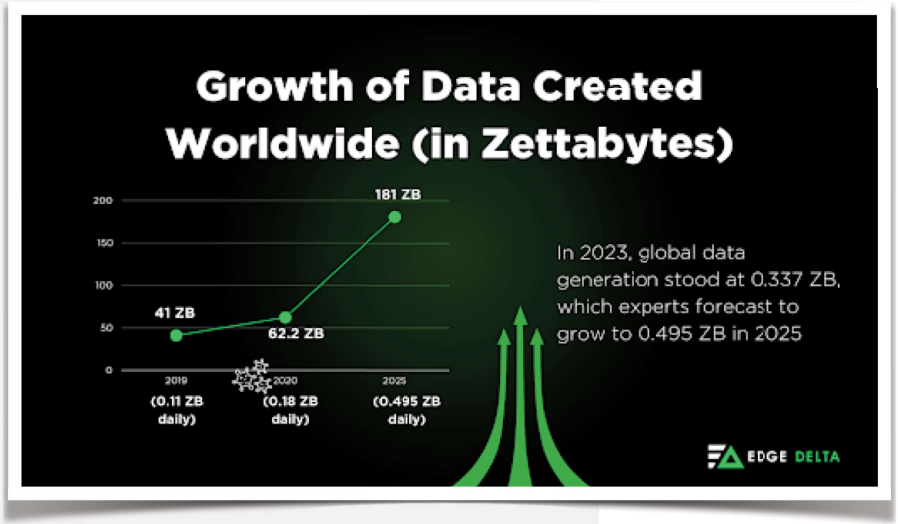
3,026,626
emails sent every second, 67% of which are spam

278,108 PETABYTES
global IP data per month by the end of 2021

230,000
new malware versions created every day

82%
share of video in total global internet traffic at the end of 2021





- In 2023, **Facebook** produced around **4 PB** on average **per day**.
- An average **IG account** uses around **9.6 GB to 14.4 GB daily**.
- With 619 million active users, **X** creates around **12 TB daily**.
- **TikTok** users spent around **840 MB per hour** on the app in 2023.
- The **YouTube** global community uses approximately **440,000 TB** daily.
- **Google** manages approximately **20 PB every day**.

Type of Content	Amount of Data Generated Daily
Videos	2.71 Hours of Videos
Images	3.2 Billion Photos Shared
Audio	1.38 Hours of Listening Session

BREACHES AND INCIDENTS

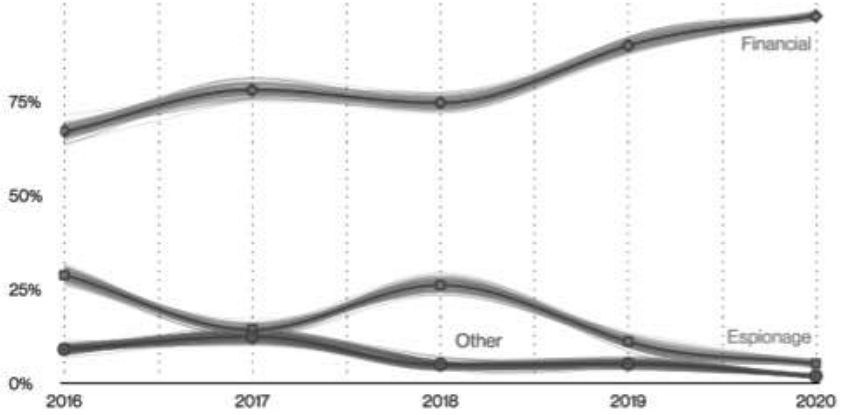


Figure 15. Top threat actor motive over time in breaches

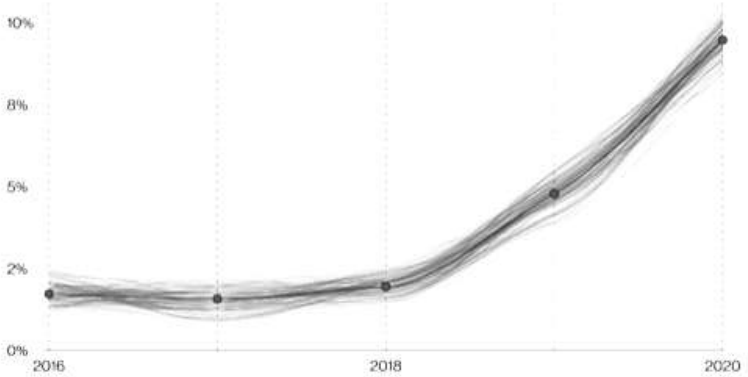


Figure 83. Ransomware in breaches over time

Summary

Northern American organizations continue to be the target of Financially motivated actors searching for money or easily monetizable data. Social Engineering, Hacking and Malware continue to be the favored tools utilized by these actors.

Frequency	13,256 incidents, 1,080 with confirmed data disclosure
Top Patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 92% of breaches
Threat Actors	External (82%), Internal (19%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (96%), Espionage (3%), Grudge (2%), Fun (1%) (breaches)
Data Compromised	Credentials (58%), Personal (34%), Other (27%), Internal (11%) (breaches)

*Verizon 2021 Data Breach Investigations Report

BREACHES AND INCIDENTS

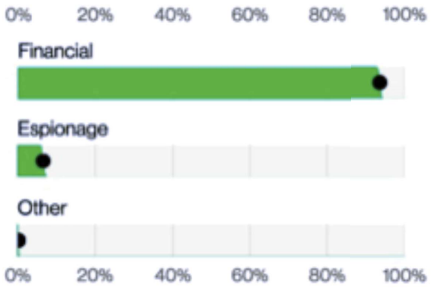


Figure 12. Threat actor motives in breaches (n=5,632)

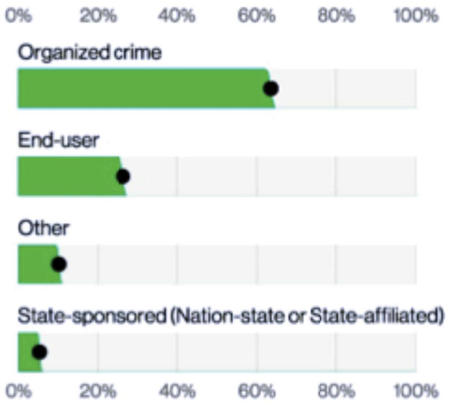


Figure 13. Threat actor varieties in breaches (n=7,921)

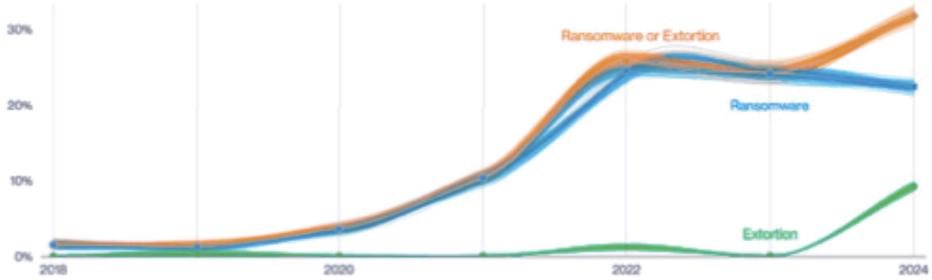
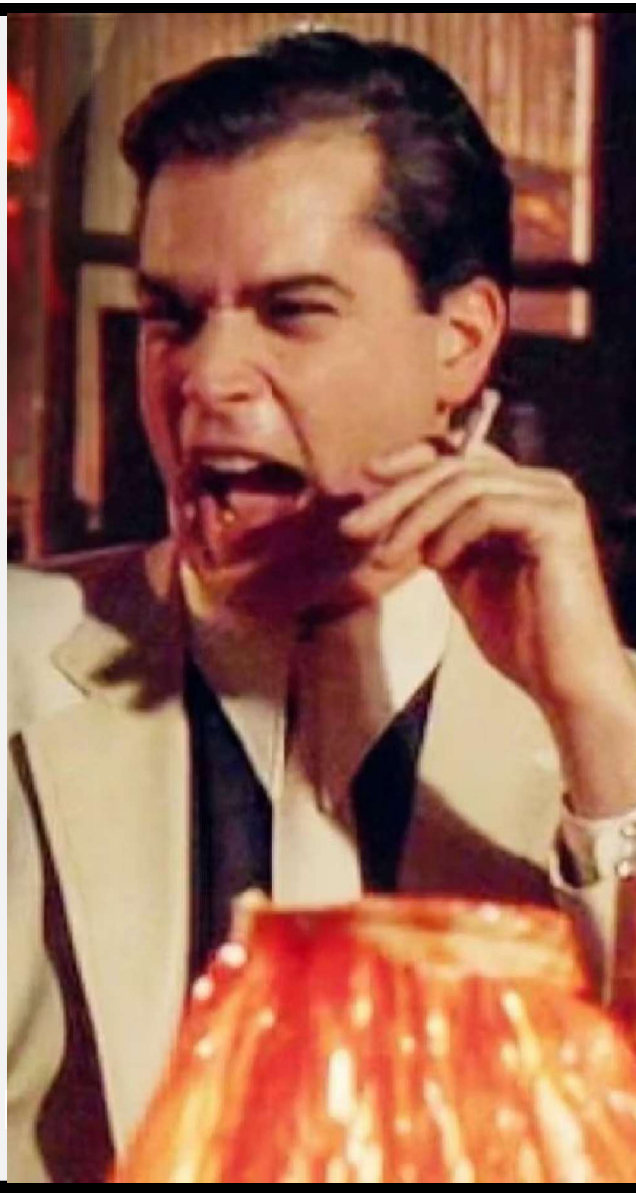


Figure 2. Ransomware and Extortion breaches over time



PATTERNS FOR SMBS, PROF. SERVICES

Small (Less than 1,000 employees)

Frequency	1,037 incidents, 263 with confirmed data disclosure
Top Patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 80% of breaches
Threat Actors	External (57%), Internal (44%), Multiple (1%), Partner (0%) (breaches)
Actor Motives	Financial (93%), Espionage (3%), Fun (2%), Grudge (1%), Other (1%) (breaches)
Data Compromised	Credentials (44%), Personal (39%), Other (34%), Medical (17%) (breaches)

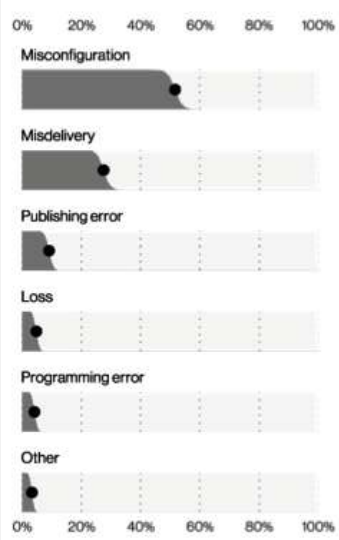


Figure 62. Top Error varieties in Miscellaneous Errors breaches (n=609)

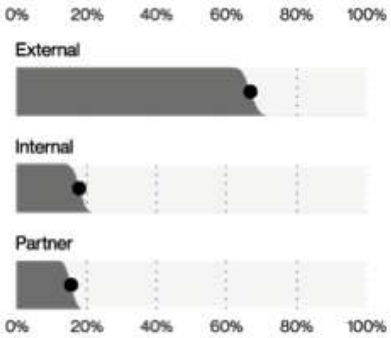


Figure 78. Discovery methods in Social Engineering incidents (n=691)

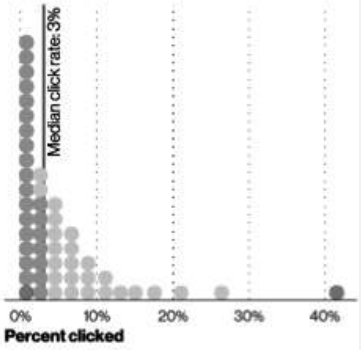


Figure 75. Click rate for organizations in their last phishing campaign (n=18,177) Each dot represents 2% of organizations.

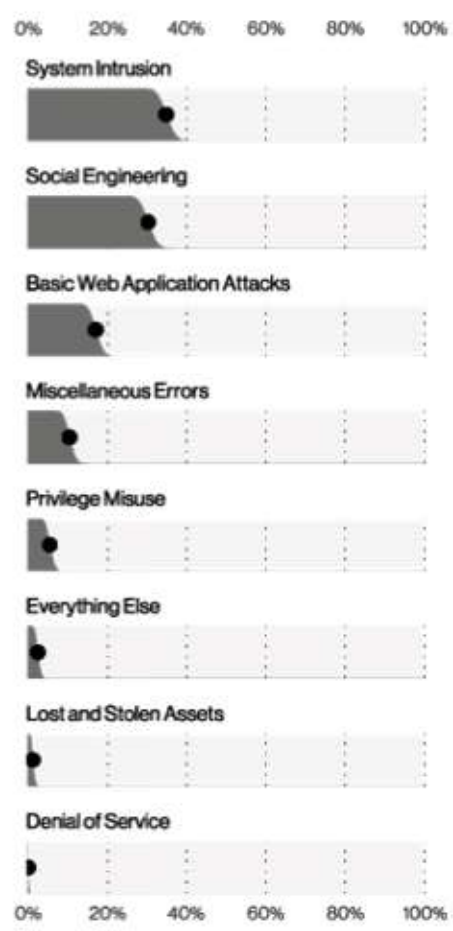


Figure 113. Patterns in Professional Services breaches (n=630)

*Verizon 2021 Data Breach Investigations Report

PATTERNS FOR SMBS, PROF. SERVICES

Figure 3. Select key enumerations in breaches

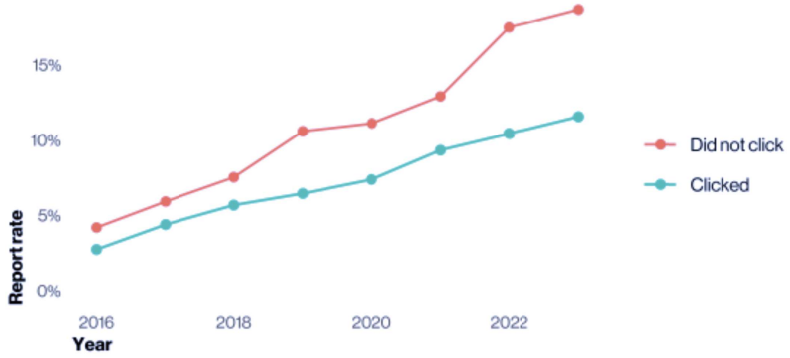


Figure 4. Phishing email report rate by click status

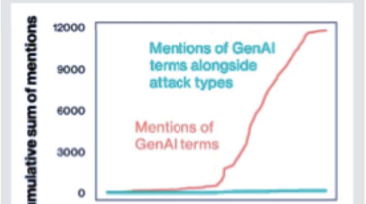


Figure 14. Cumulative sum of GenAI in criminal forums

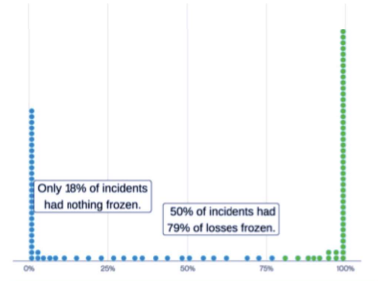


Figure 37. Percent of losses frozen for recovery

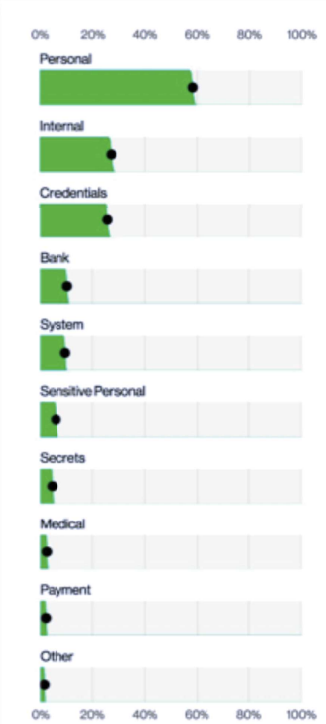
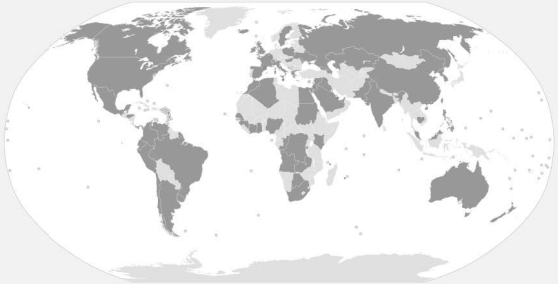


Figure 24. Top Confidentiality data varieties in breaches

*Verizon 2024 Data Breach Investigations Report

WHY, YOU ASK?

Everyone is now a target of evolving threat actors



Monetizing information

Account credentials are easy to steal, but it requires further work to monetize those data elements before controls take effect. What's more appealing is…

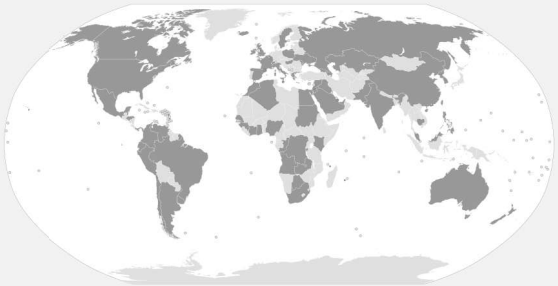
- Valuable information
  - Trade secrets and intellectual property
  - Financial data and M&A plans
  - Personal details (browsing data)
- Extortion, i.e., ransomware
- Bitcoin mining
- Industrial espionage
- Reputational harm (e.g., DDoS attacks)

Crime *does* pay

- The average cost of a data breach is $3.86 million as of 2020. (IBM)
- The average ransomware payment rose 33% in 2020 over 2019, to $111,605. (Fintech News)
- The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)
- The average cost of a malware attack on a company is $2.6 million. (Accenture)
- The most expensive component of a cyber attack is information loss at $5.9 million. (Accenture)
- The average cost per lost or stolen record per individual is $146. (IBM)
- Data breaches cost enterprises an average of $3.92 million. (CSO Online)

WHY, YOU ASK?

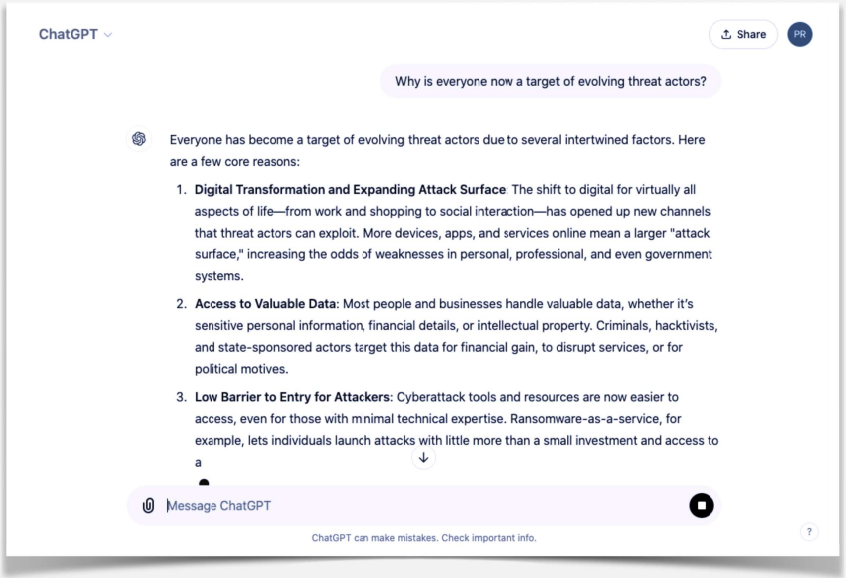
Everyone is now a target of evolving threat actors



Monetizing information

- **Expanded Attack Surface**: More devices and apps online increase vulnerabilities.
- **Valuable Data**: Individuals and businesses handle sensitive data—ideal for cyber criminals.
- **Low Barrier to Entry**: Tools for cyberattacks are widely available, even for non-experts.
- **Remote Work Risks**: Personal networks are easier to exploit than corporate systems.
- **AI-Driven Attacks**: AI enhances phishing and impersonation, making detection harder.
- **Geopolitical Motivations**: Ideological and state-sponsored attacks target broader audiences.

ChatGPT



NO TAXATION WITHOUT INFORMATION

Tax data makes a prime target

- Many federal agencies have been hit with damaging cyberattacks in recent years, including the Office of Personnel Management, the Justice Department, the Pentagon, and the White House.
- The IRS has also suffered attacks
  - Ideal target for hackers seeking to steal personal information and money
    - Some people simply want to wreak havoc by destroying data (e.g., thieves, nation state actors, etc.)
  - The IRS collects information on our income sources, family structure, health information, housing data, small business details, educational situation, retirement finances, and many other things
  - In 2015, the IRS launched the "Get Transcript" service, enabling taxpayers to view this information online. Within the first few months of the service, hackers stole personal information from about 724,000 taxpayer accounts.
- Politicians encourage the IRS to improve "customer service," which encourages more online interaction. And politicians push to close the "gap" of taxes owed but not collected, prompting the agency to demand more data from individuals and businesses.

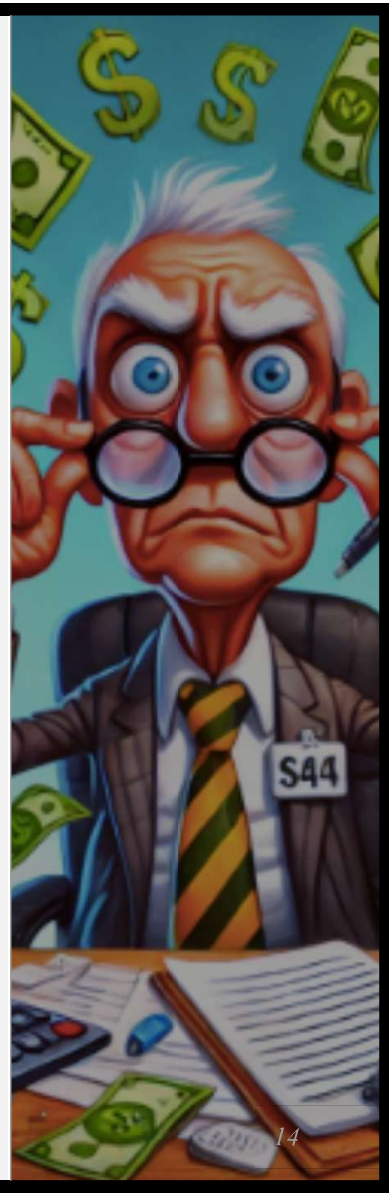
NO TAXATION WITHOUT INFORMATION

Tax data makes a prime target

- **IRS Direct File Program (2025)**
  - Allows taxpayers to file directly with the IRS, bypassing third parties
  - Enhances data collection for better service and experience IRS

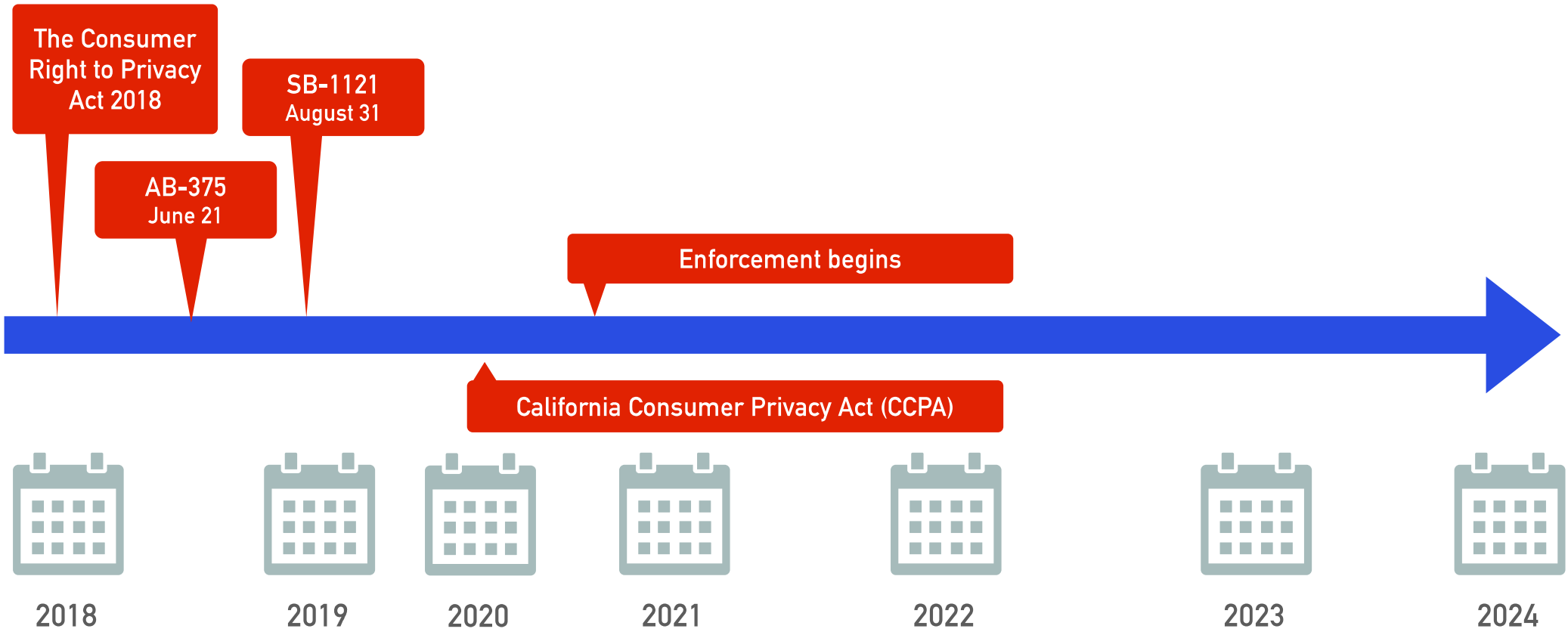
- **Paperless Processing Initiative**
  - Nearly all documents can be filed digitally by 2025
  - Faster processing, lower costs, secure digital storage IRS

- **Corporate Transparency Act Compliance**
  - IRS may use corporate ownership data to identify tax liabilities and address fraud
  - Contributes to transparency in business structures
  - For each beneficial owner and company applicant, the report must provide **full legal names**, **current residential or business addresses**, **dates of birth**, and a unique identifier such as a **passport, driver's license, or similar document number**.



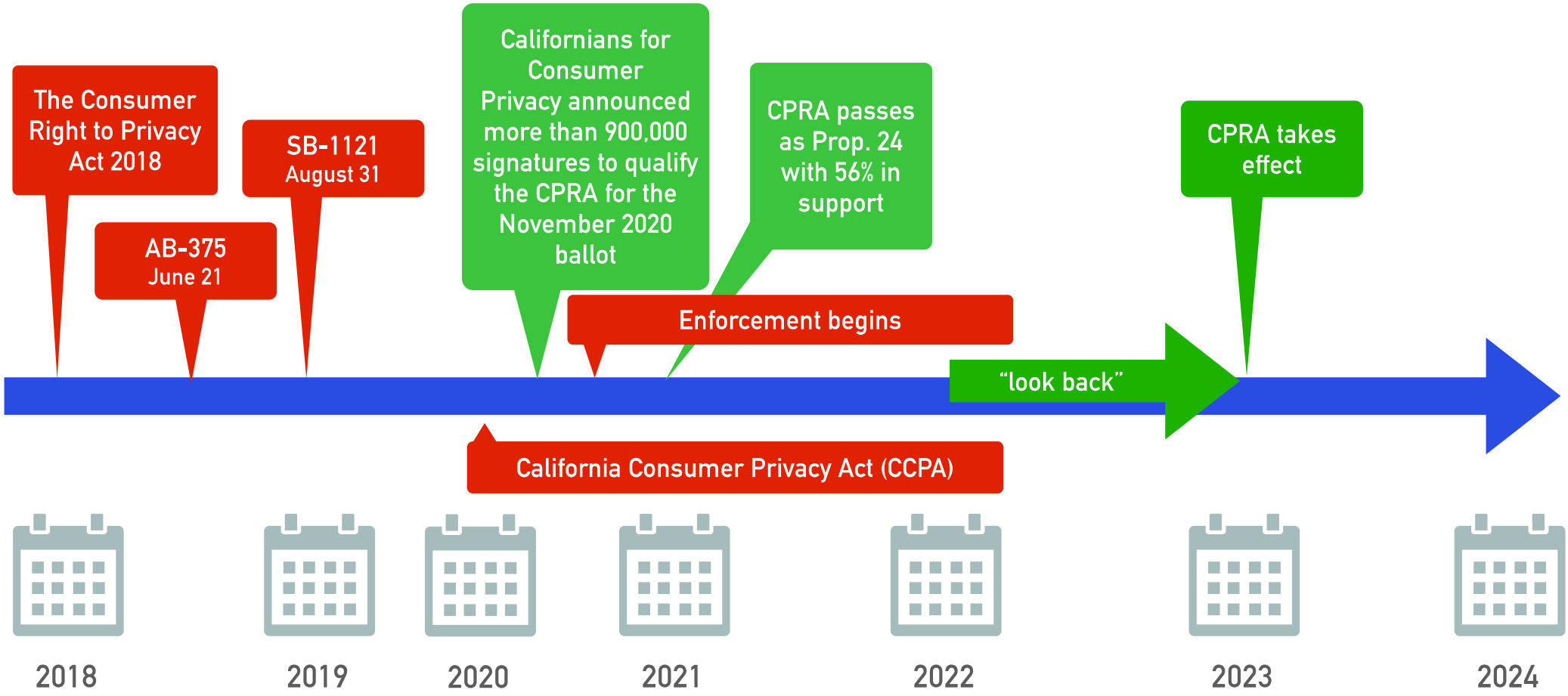
USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



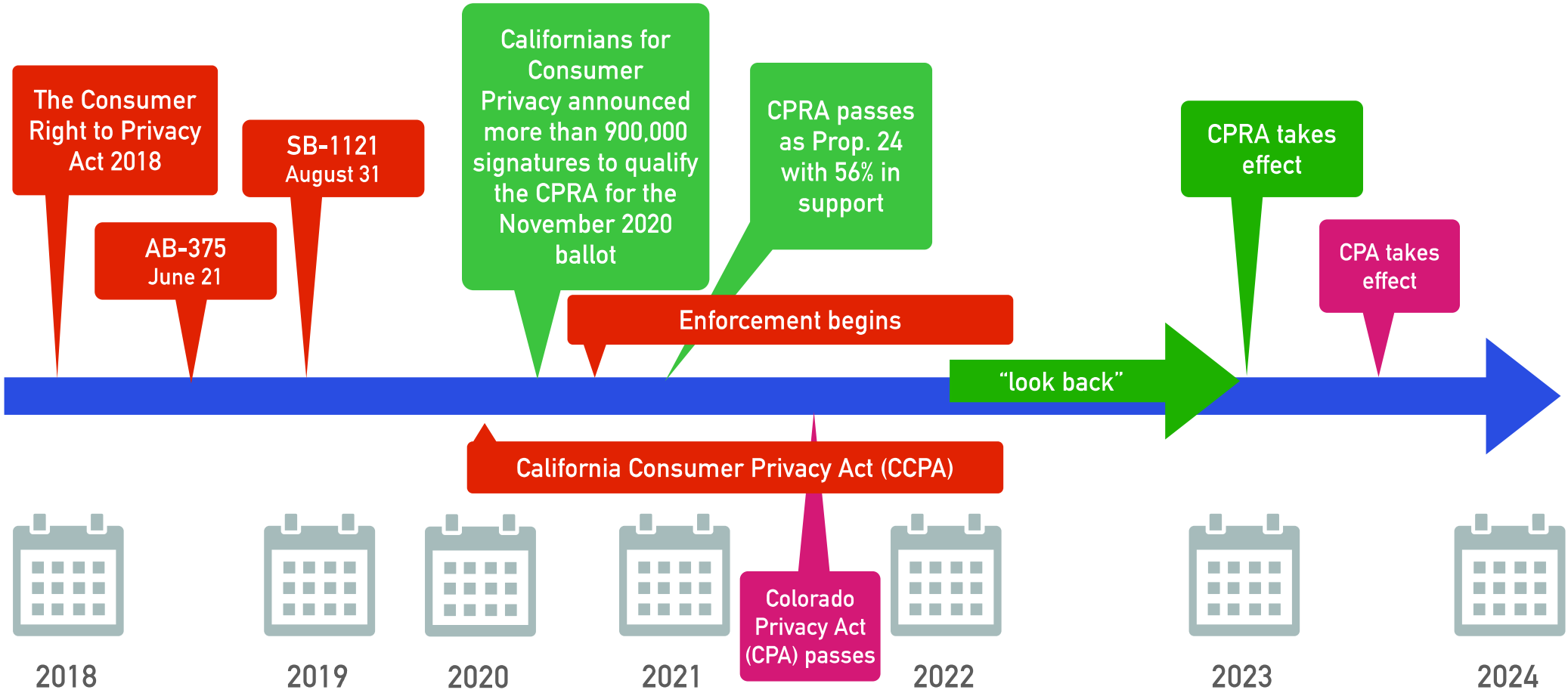
USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



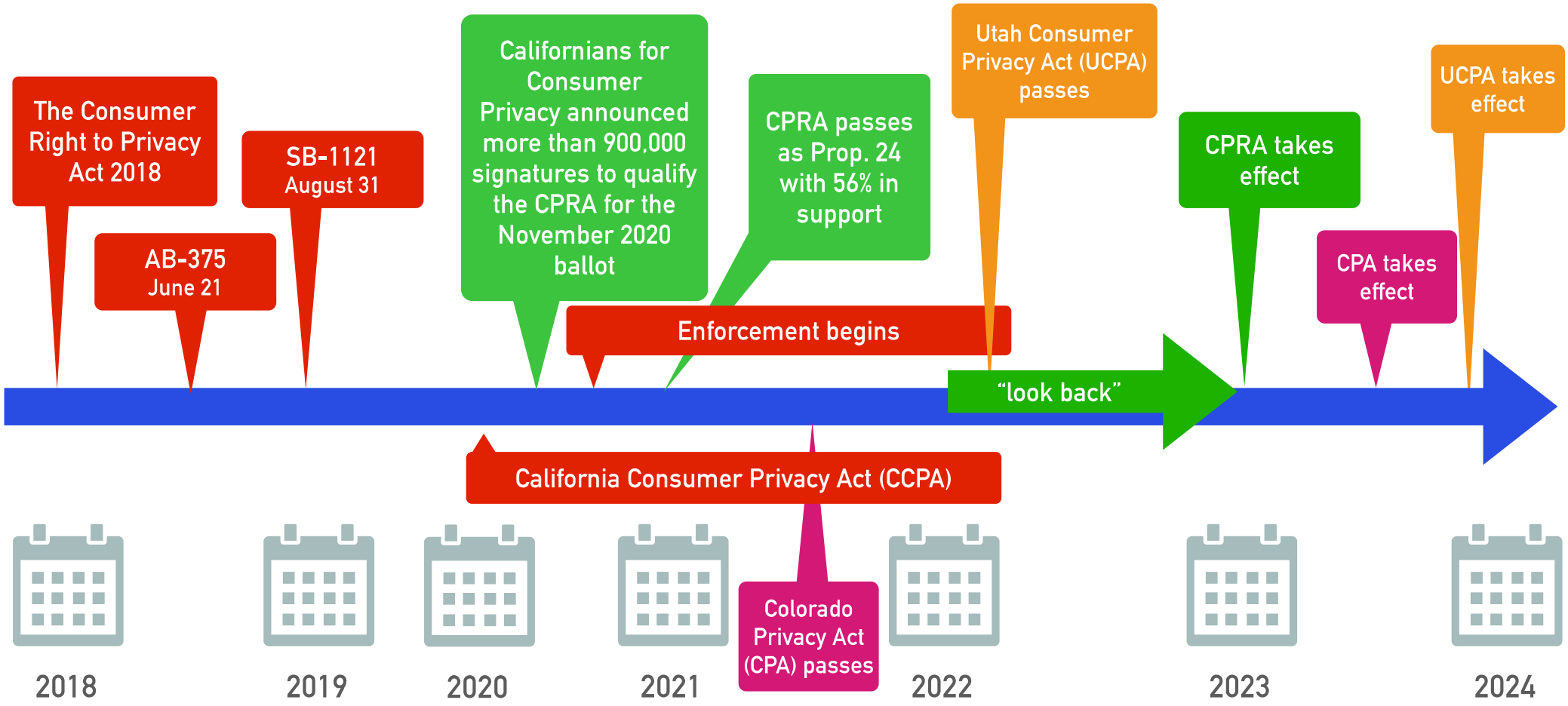
USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



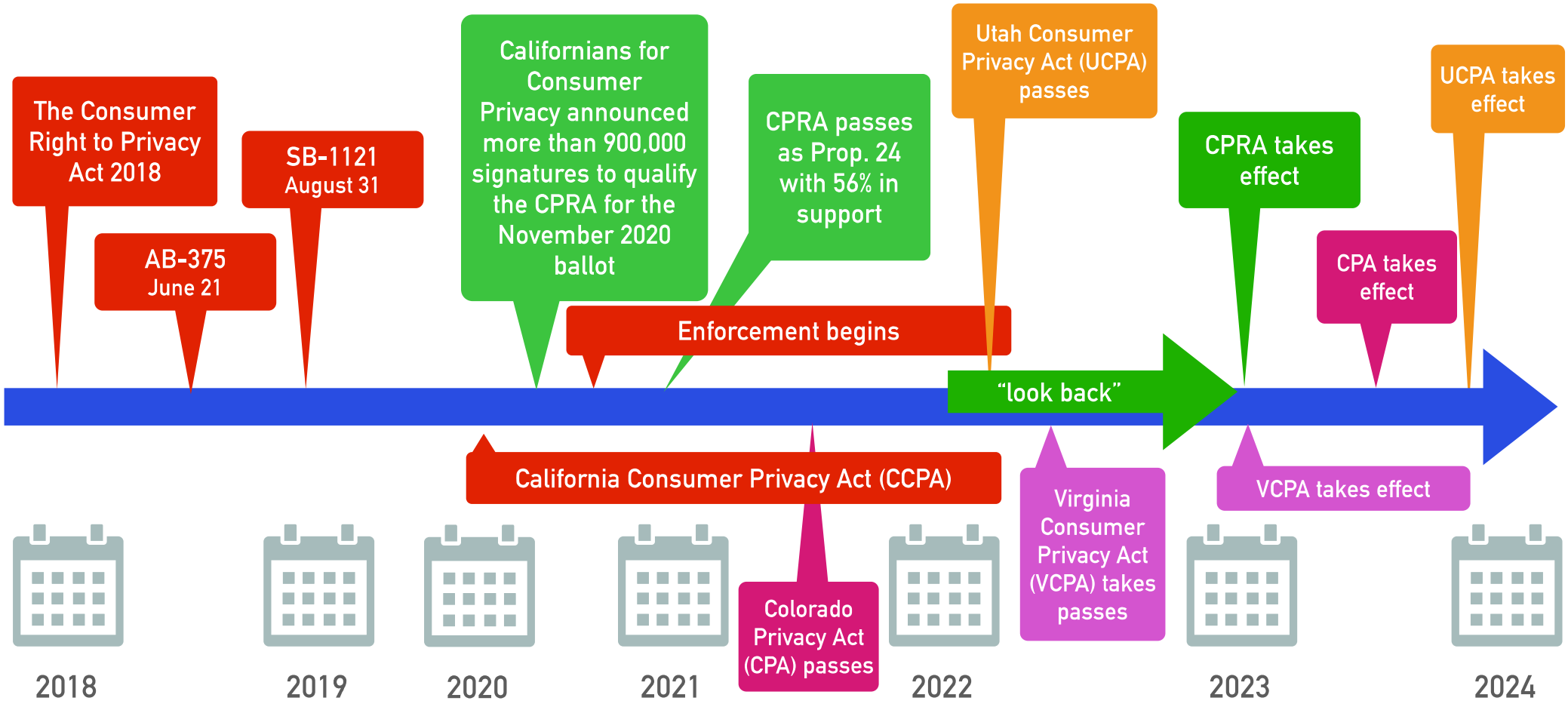
USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



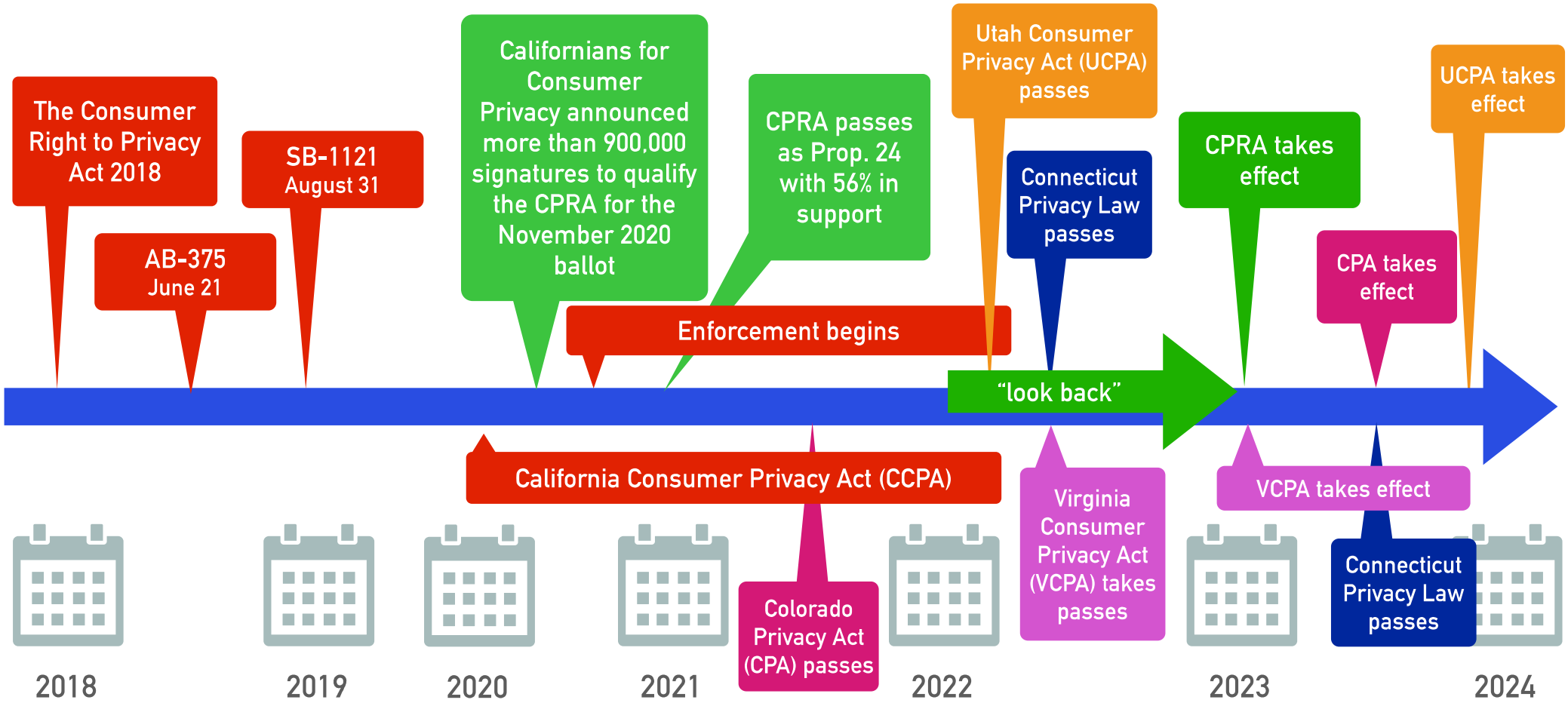
USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON



USA STATE CONSUMER PRIVACY LAWS

A BRIEF HISTORY LESSON

Utah Consumer Privacy Act (UCPA) passes

Connecticut Privacy Law passes

CPRA takes effect

CPA takes effect

UCPA takes effect

N.M. Stat. Ann. § 1-19-26.4 (proposed as HB 182) enacted

"look back"

Virginia Consumer Privacy Act (VCPA) takes passes

VCPA takes effect

Connecticut Privacy Law passes

CO SB204-205 Consumer Protections for Artificial Intelligence passes

CO SB204-205 takes effect

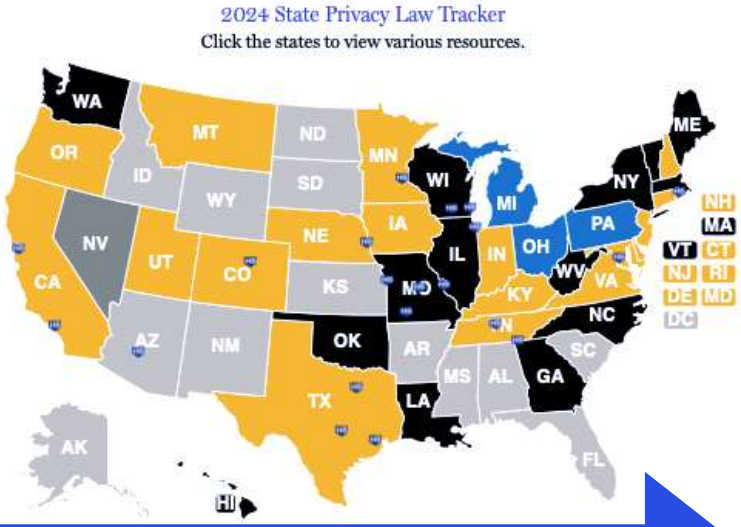
22

2023

2024

2025

2026



Who do these privacy laws apply to?

Often applies to controllers that conduct business in the state

~or~

produce or deliver commercial products or services that are intentionally targeted to state residents and that either:

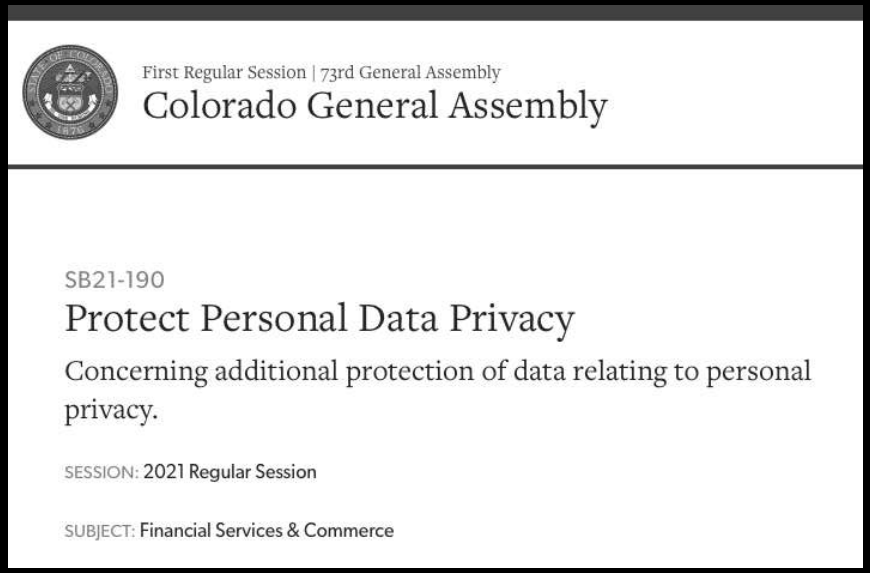
- *control or process personal data of (100,000) consumers or more per calendar year; or*
- *derive revenue or receive a discount on the price of goods or services from the sale of personal data and control or process the personal data of (25,000) consumers or more.*

What are the main obligations?

- collection of personal data must be *adequate*, *relevant*, and *limited* to what is reasonably necessary in relation to its specified purposes;
- taking *reasonable measures* to secure personal data;
- requiring consent to process a consumer's sensitive data;
- provide consumers with a reasonably clear, accessible, and meaningful privacy notice including:
  - *the categories of personal data collected or processed;*
  - *the purpose for which personal data will be collected and processed;*
  - *the categories of personal data shared with third parties, if any;*
  - *the categories of third parties with whom the data is shared; and*
  - *how and where consumers may exercise their data subject rights, including the controller's contact information and how to appeal.*

Colorado Privacy Act

SB21-190



First Regular Session | 73rd General Assembly

Colorado General Assembly

SB21-190

Protect Personal Data Privacy

Concerning additional protection of data relating to personal privacy.

SESSION: 2021 Regular Session

SUBJECT: Financial Services & Commerce

Who do these AI laws apply to?

Applies to developers and deployers of high-risk AI systems:

- *Developers: Businesses in Colorado that develop or significantly modify certain AI models or systems; or*
- *Deployers: Businesses in Colorado that deploy specific high-risk AI systems.*

What are the main obligations?

- *Risk Management Policy*: Deployers must implement a risk mgmt. policy and program specifically for high-risk AI systems.
- *Impact Assessment*: An impact assessment of the high-risk system is required to evaluate potential risks.
- *Annual Review*: Deployers must conduct annual reviews of their high-risk systems to ensure they are not causing algorithmic discrimination.
- *Consumer Notification*: Consumers must be notified when a high-risk system is involved in making consequential decisions about them.
- *Data Correction Opportunities*: Consumers should have the chance to correct any inaccurate personal data processed by the AI system that influenced consequential decisions.
- *Public Disclosure*: Deployers must make a public statement about the types of high-risk systems they operate, the risks associated with them, and the data they collect.
- *Reporting Algorithmic Discrimination*: If a deployer discovers algorithmic discrimination, they must disclose this to the attorney general within 90 days.

Colorado AI Act

SB204-205

Second Regular Session | 74th General Assembly
Colorado General Assembly

INTERIM SCHEDULE BILLS LAWS LEGISLATORS COMMITTEES INITIATIVES BUD

SB24-205

Consumer Protections for Artificial Intelligence

Concerning consumer protections in interactions with artificial intelligence systems.

SESSION: 2024 Regular Session

SUBJECTS: Business & Economic Development, Labor & Employment, Telecommunications & Information Technology

BILL SUMMARY

On and after February 1, 2026, the act requires a developer of a high-risk artificial intelligence system (high-risk system) to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system. There is a rebuttable presumption that a developer used reasonable care if the developer complied with

WHERE TO START?

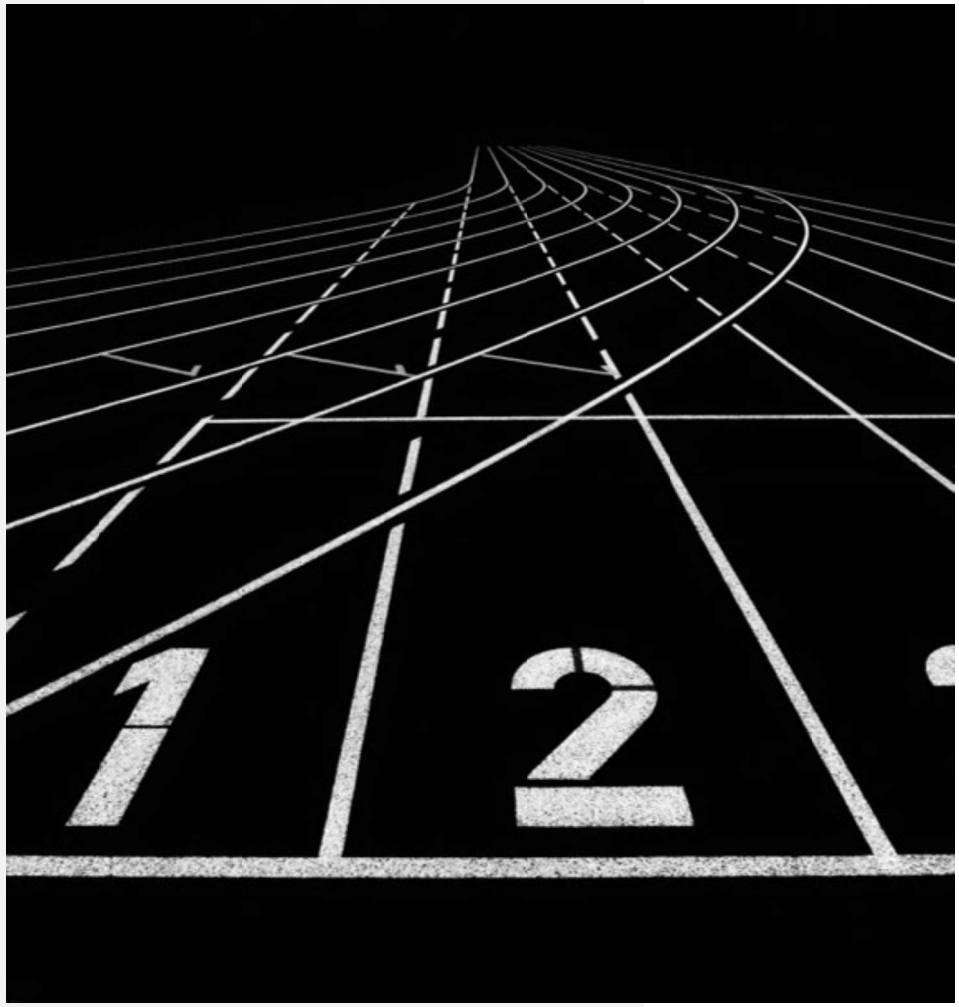
1. What information do I need to protect?
   IT assets, paper files, admin systems

2. Where are my current gaps in compliance?
   Compare existing systems to legal or competitor benchmarks

3. What are my urgent priorities?
   Develop a plan based on managed risk

4. Where (and what) can I automate?
   People, processes, technology

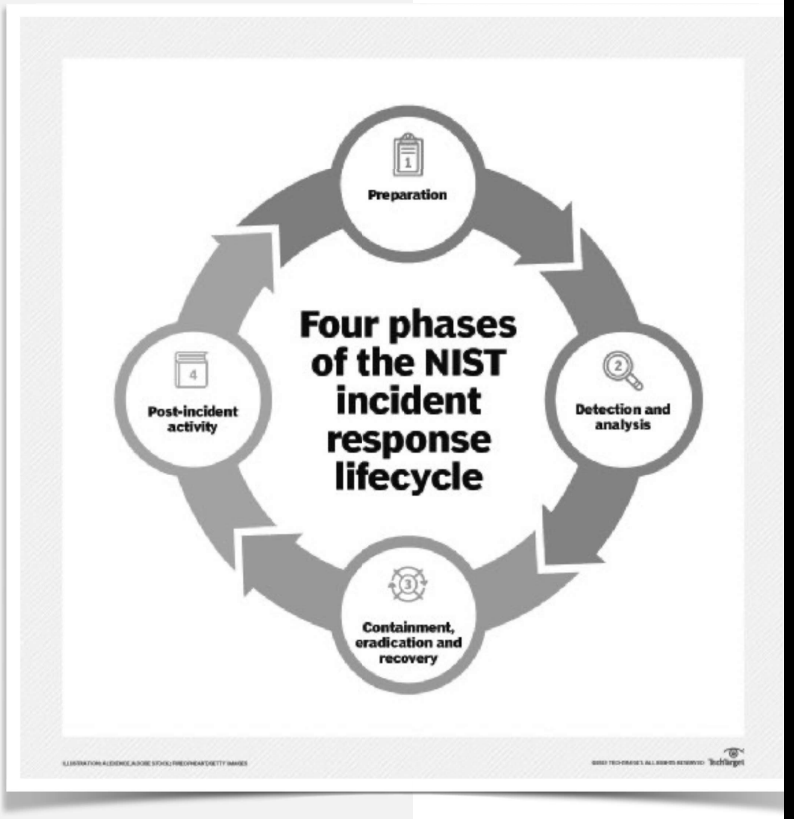
5. Where else can I get help?
   Vendors/partners



Preparation

CYBERSECURITY LIFECYCLE - PREPARE

- ***Assess**…your current environment*
  - Data mapping
    - Required for compliance with laws like the EU's GDPR
    - Identifies 'sensitive' data or high-risk information
  - Gap analysis - industry standards for information security
    - ISO 27001; ISO 42001
    - SOC 2, Type II
    - NIST 800-53 / 800-171; NIST AI RMF
    - CMMC
- ***Plan**…for the worst (pray for the best!)*
  - Bolster cyber defenses
    - Review technical sec. measures (e.g., SIEM, EDR, patch & vuln. mgmt.)
    - Build a response team (InfoSec response; Customer Care; Legal + team)
  - Consider cyber insurance
    - Provides financial coverage for costs associated w/computer hacking events, data breaches, ransomware, and related computer system failures
    - Review coverage, requirements



SearchSecurity - TechTarget

Form **1040** Department of the Treasury—Internal Revenue Service (99)

U.S. Individual Income Tax Return

2021 | OMB No. 1545-0074 | IRS Use Only—Do not write or staple in this space.

Filing Status Check only one box.
☐ Single ☐ Married filing jointly ☐ Married filing separately (MFS) ☐ Head of household (HOH) ☐ Qualifying widow(er) (QW)
If you checked the MFS box, enter the name of your spouse. If you checked the HOH or QW box, enter the child's name if the qualifying person is a child but not your dependent ▶

Your first name and middle initial	Last name	**Your social security number**
If joint return, spouse's first name and middle initial	Last name	**Spouse's social security number**

Home address (number and street). If you have a P.O. box, see instructions.	Apt. no.	**Presidential Election Campaign** Check here if you, or your spouse if filing jointly, want $3 to go to this fund. Checking a box below will not change your tax or refund. ☐ **You** ☐ **Spouse**
City, town, or post office. If you have a foreign address, also complete spaces below.	State / ZIP code	
Foreign country name / Foreign province/state/county / Foreign postal code		

At any time during 2021, did you receive, sell, exchange, or otherwise dispose of any financial interest in any virtual currency? ☐ **Yes** ☐ **No**

Standard Deduction **Someone can claim:** ☐ You as a dependent ☐ Your spouse as a dependent
☐ Spouse itemizes on a separate return or you were a dual-status alien

Age/Blindness **You:** ☐ Were born before January 2, 1957 ☐ Are blind **Spouse:** ☐ Was born before January 2, 1957 ☐ Is blind

Dependents (see instructions): If more than four

(1) First name Last name	(2) Social security number	(3) Relationship to you	(4) ✔ if qualifies for (see instructions): Child tax credit	Credit for other dependents
			☐	☐

Form **1040** Department of the Treasury—Internal Revenue Service (99) **U.S. Individual Income Tax Return** **2021** OMB No. 1545-0074 IRS Use Only—Do not write or staple in this space.

Filing Status Check only one box. ☐ Single ☐ Married filing jointly ☐ Married filing separately (MFS) ☐ Head of household (HOH) ☐ Qualifying widow(er) (QW)

If you checked the MFS box, enter the name of your spouse. If you checked the HOH or QW box, enter the child's name if the qualifying person is a child but not your dependent ▶

Your first name and middle initial	Last name	**Your social security number**
If joint return, spouse's first name and middle initial	Last name	**Spouse's social security number**

Home address (number and street). If you have a P.O. box, see instructions.	Apt. no.	**Presidential Election Campaign** Check here if you, or your spouse if filing jointly, want $3 to go to this fund. Checking a box below will not change your tax or refund. ☐ **You** ☐ **Spouse**
City, town, or post office. If you have a foreign address, also complete spaces below.	State / ZIP code	
Foreign country name / Foreign province/state/county / Foreign postal code		

At any time during 2021, did you receive, sell, exchange, or otherwise dispose of any financial interest in any virtual currency? ☐ **Yes** ☐ **No**

Standard Deduction **Someone can claim:** ☐ You as a dependent ☐ Your spouse as a dependent ☐ Spouse itemizes on a separate return or you were a dual-status alien

Age/Blindness **You:** ☐ Were born before January 2, 1957 ☐ Are blind **Spouse:** ☐ Was born before January 2, 1957 ☐ Is blind

Dependents (see instructions): If more than four

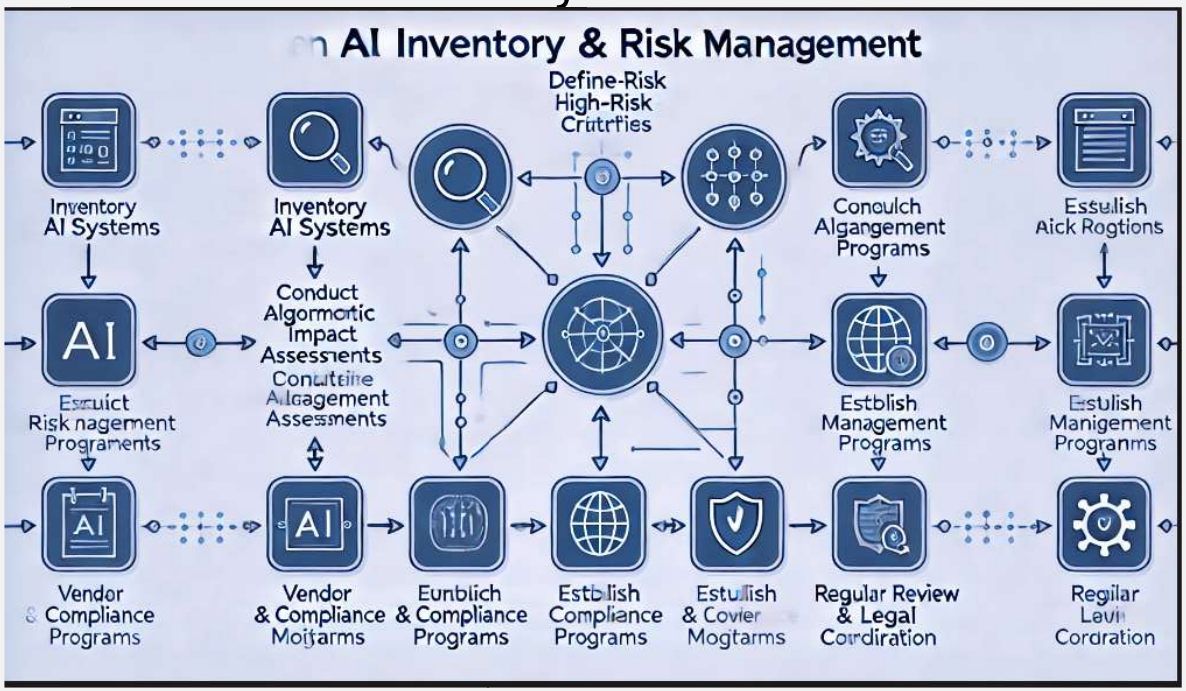
(1) First name	Last name	(2) Social security number	(3) Relationship to you	(4) ✔ if qualifies for (see instructions): Child tax credit	Credit for other dependents
				☐	☐

Personally Identifiable Information	Name & Contact Information	Personal Characteristics & Health & Ins Acct Information	Financial Data & Employment Information
Social Security # State-issued ID # Driver's license # Passport # Mother's Maiden Name Credit history Criminal history	Initials Address Telephone number E-mail address Mobile number Date of birth EFINs / PTINs / CAF #	Age Gender Marital status Nationality Insurance account # Prescriptions Medicare and Medicaid info	Credit, ATM, debit card #s Bank Accounts Security/Access Codes Passwords Income/Salary Service fees Compensation info Background check info

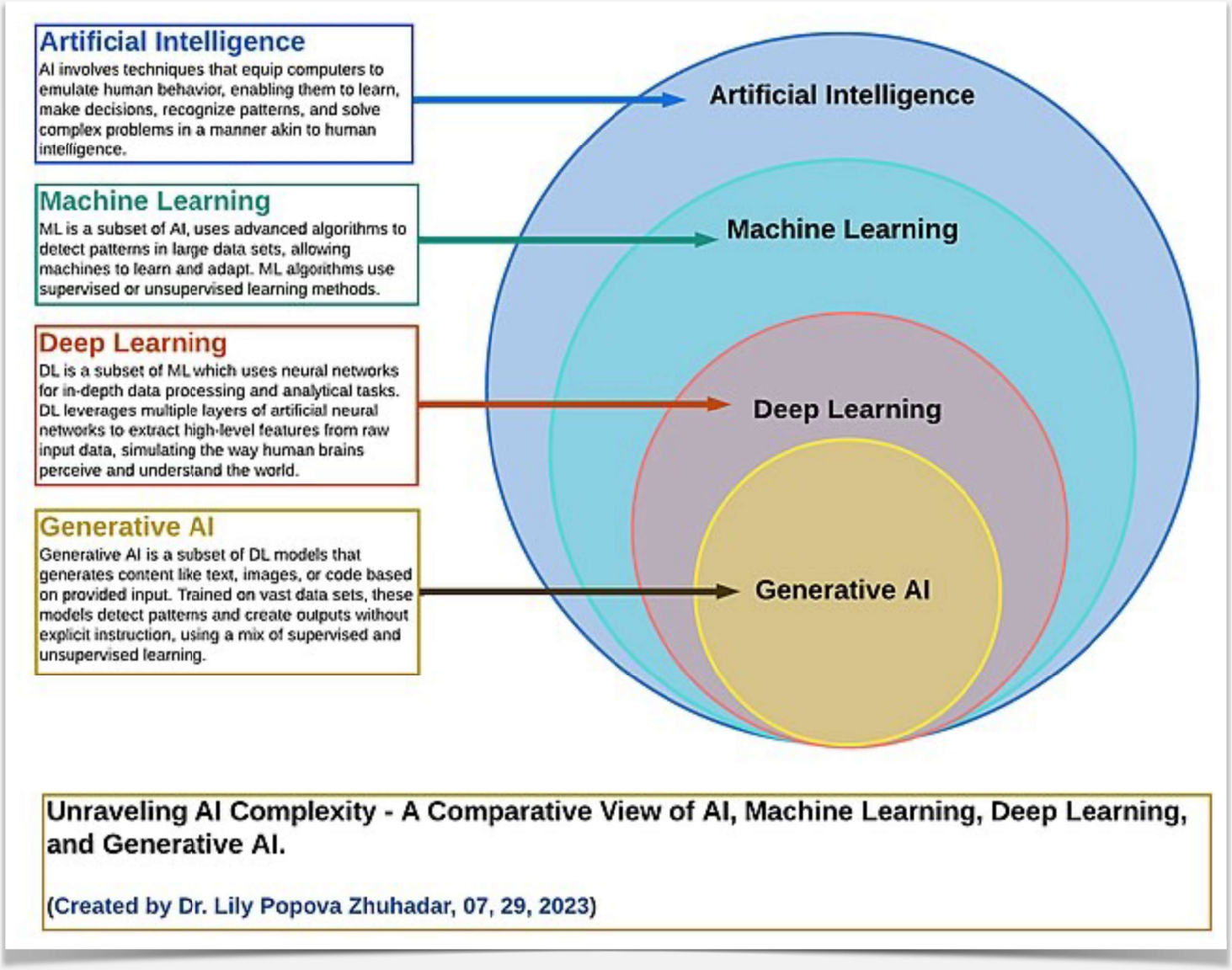
Business function	Purpose of processing	Business Critical	Source of the data (external)	Source of the data (internal)	Categories of personal data	Types of personal information
Taxes	Outside records on sales and use taxes, telecommunications taxes, property taxes, federal, state and local tax returns, payroll and payroll taxes, billing and accounting records	Tax consultant Payroll provider	Finance Team	B2B contact info	Name, company address	Finance Team ("R" drive)
Company Insurance	Insurance policies (D&O, E&O, Workers Comp, and General Liability policies, applications, quotes, audits and adjustments, annual insurance loss summary reports, certificates of insurance, insurance claims files and correspondence)	Insurance Carrier	Finance Team	B2B contact info	Name, Company Address; Contract number	FinanceTeam (policies and COI's) Sales Team (COI's) Legal Team (COI's)
Financial Planning & Analysis	Financial planning (budgets, revenue data, sales data, budgeting and trending, averages, forecasting, marketing discounts, ROI data, models, data, analysis, P&L reviews, reports, ad hoc reporting, management reporting)	ERP System Third party vendor (usage and sales metrics)	Finance Team AR Stats - Usage	B2B contact info	Name	Finance Team Senior management as needed
Employee payroll	Employee payroll (deductions, registers, FLSA, comps, time sheets, wage and tax registers, payroll tax returns, check deposits, reversals, direct deposit, payroll related forms, W-4s, W-2s); commissions, bonuses, incentives, awards, board compensation approvals; unemployment wage records, reports and tax returns	Employee bank State (taxes)	Data subject (employee)	Payroll info	Name, Role/Title	Finance Team
Equity management	stock purchase plan records (option grants, election records, exercise forms, vesting, expiration records, pre-clearances, timing windows, board records, FRS Equity records, DLA/UBS records, AST stock sale records)	N/A	Data subject (employee)	Employee contact info	Name, email address, options granted	Employees
Payroll reporting	backup materials (payroll withholding records); reconciliations	payroll system	Data subject (employee) HR Team	Employee payroll info	Names, company address, email address, phone number, SS#, job title, wage/ compensation	Finance
Financial records	General ledger and associated documentation (subledgers, journal and subjournal entries, postings, reconciliations, spreadsheets, servers SAP extracted data, accounts receivable invoices, cash receipts, aging and allowance calculations, fees, deposits, receipts, accounts payable invoices, master files, W-9s, e-transfers, wire records, employee expense reports, vouchers, 1099 forms and reports, travel and entertainment details, payment registers, reconciliations, credit cards, fixed assets, adjustments invoices, asset write up, capital property, inventory records travel and entertainment receipts, depreciation reconciliations, depreciation schedules, credit facilities, charitable contributions); audited financial reports; External technical accounting memos	Third - parties (incl. vendors & customers)	All departments as applicable	B2B banking info	Names, company address, email address, phone number, banking information	Finance Team Senior management as needed

CYBERSECURITY LIFECYCLE - PREPARE

- *Inventory AI Systems*
  - List all AI/ML tools in use, especially those in decision-making and client services.
  - Look for systems that process sensitive data, automate decisions, or could impact individuals financially.



- *Establish Risk Management Programs*
  - Set up programs to monitor, disclose, and document risks, focusing on transparency with clients.
    - *Conduct Algorithmic Impact Assessments (AIAs)*
      - Assess potential biases, impacts on protected groups, and risk of errors for each high-risk system.
    - *Vendor & Compliance Monitoring*
      - Require third-party vendors to document their compliance practices and monitor evolving legal requirements.
    - *Regular Review & Legal Coordination*
      - Ensure continuous alignment with regulatory standards and legal guidance on AI risks.



Unraveling AI Complexity - A Comparative View of AI, Machine Learning, Deep Learning, and Generative AI.

(Created by Dr. Lily Popova Zhuhadar, 07, 29, 2023)


Detection &
Analysis
www.h.hospital.com
HOSPITAL
We provide high quality medical services with trained specialists and advanced medical equipment. Our team is completely involved with the patients delivering a comprehensive range of services ranging from primary to tertiary care, from consultation and diagnosis, planning and executing treatment, and following-up results.
Home
About Us
Patient Services
Find a Doctor
Our Centers
Contact Us
We have almost 20 tenants ranging from daily convenience stores, banks and popular international chains. In addition, there is a selection of retail and food and beverage outlets. We provide high quality medical services with trained specialists and advanced medical equipment.

CYBERSECURITY LIFECYCLE - DETECTION & ANALYSIS

- ***Identify**…threats and vulnerabilities*
  - Monitory cyber-advisory services
    - CISA - Cybersecurity and Infrastructure Security Agency (CISA)
    - OWASP - nonprofit that produces articles, documents, tools, and technologies in the field of web application security.
  - Scan for chinks in the armor
    - Vulnerability scanning - assess computers, networks, or applications for known weaknesses (tools)
    - Penetration testing - simulated cyber attack against your system to check for exploitable vulnerabilities
    - Phishing simulations - the fraudulent practice of sending emails inducing individuals to reveal personal information
      - Smaller organizations (1–250 employees) have the highest targeted malicious email rate at 1 in 323. (Symantec)
- ***Monitor**…risks associated with staff*
  - 30% of data breaches involve internal actors. (Verizon)
  - On average, every employee has access to 11 million files. (Varonis)
    - 17% of all sensitive files are accessible to all employees. (Varonis)
  - About 60% of companies have over 500 accounts with non-expiring passwords. (Varonis)
  - The average annual security spending per employee increased from $2,337 in 2019 to $2,691 in 2020. (Deloitte)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY LIFECYCLE - DETECTION & ANALYSIS

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

- *Continuous Monitoring of Model Behavior*
  - Implement **anomaly detection** to identify **unusual model behavior** or **outputs** that may signal an attack or malfunction.
- *Performance Deviation Alerts*
  - Establish **benchmarks** and thresholds for metrics like **accuracy**, precision, and **recall**. **Trigger alerts when performance deviates** from expected levels.
- *Automated Log Analysis*
  - Utilize **AI-powered log analysis** to **spot patterns of abnormal behavior** (e.g., input data anomalies) that could indicate attacks or **emerging model bias**.
- *Incident Triage for AI-Specific Threats*
  - Assess incident severity based on the model's impact on critical decisions (e.g., financial or healthcare-related) and **prioritize high-impact risks** to users.

CYBERSECURITY LIFECYCLE - DETECTION & ANALYSIS

Issue reporting

- How are issues reported and recorded?
- **Event** vs. **incident** vs. **breach** ("*knowledge*")
- Begin investigation

Collect evidence

- Record key details (e.g., date/time, data affected, etc.)
- Evidence must maintain forensic value in case of legal action
- Insurance broker or cyber-carrier may require early notification

Initiate formal response plan

- Assemble the pre-identified incident response team
- Classify risk level; alert staff as appropriate
- Prepare & review notification procedures


Respond

CYBERSECURITY LIFECYCLE - CONTAINMENT

Containment Protocols

Set protocols for rolling back or isolating malfunctioning models to prevent broader service disruption.

Model retraining

- Retrain degraded models using fresh data or redeploy previously verified versions.

Data validation techniques

- Validate data to scrub or replace corrupted datasets
- Apply fairness interventions (e.g., re-sampling data, parameter adjustments) if bias is detected.

INCIDENT RESPONSE LIFECYCLE - CONT.

Eradicate

- Completely remove the threat. Extra validations should be performed to ensure the issue / vuln. cannot reoccur.
- Once confirmed, operating procedures may be returned to normal.

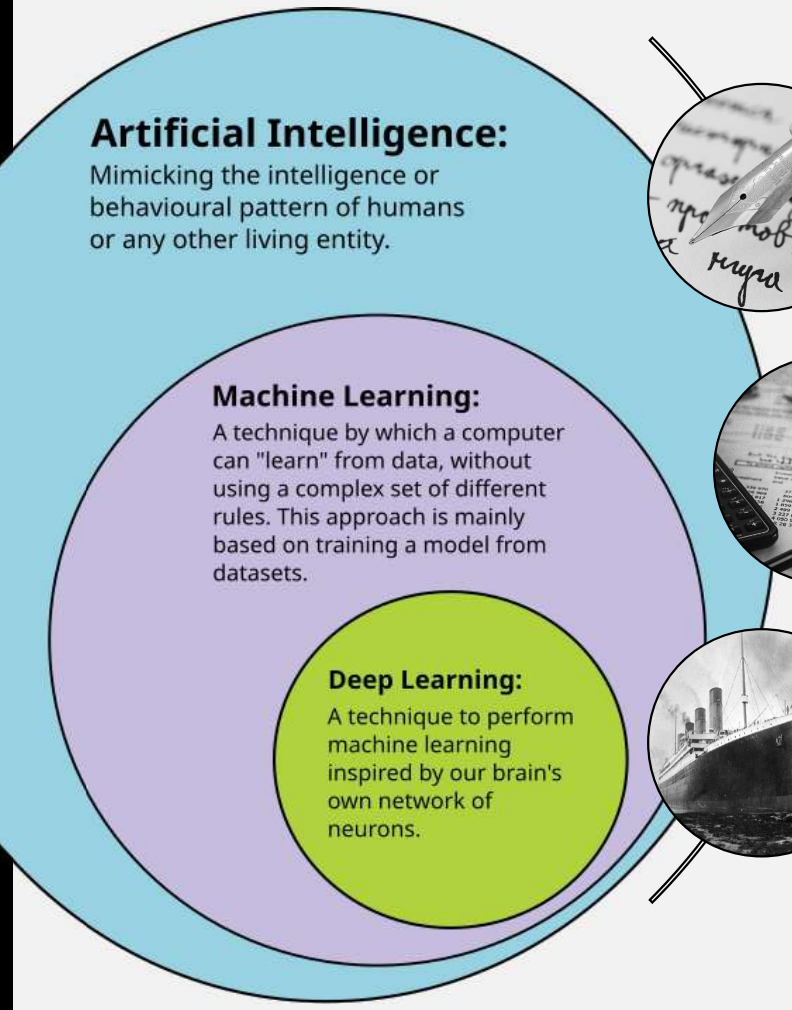
Recover

- Restore business operations in sequential order
- Debrief with Disaster Recovery Team, Legal, HR, Marketing

Report

- *Internal Communication - awareness, communication guidelines*
- *External Communication - customers, media relations*
- *Breach Notification - regulators (e.g., Atty. Gen.), data subjects*

AFTER THE INCIDENT: FOLLOW-UP



Documentation

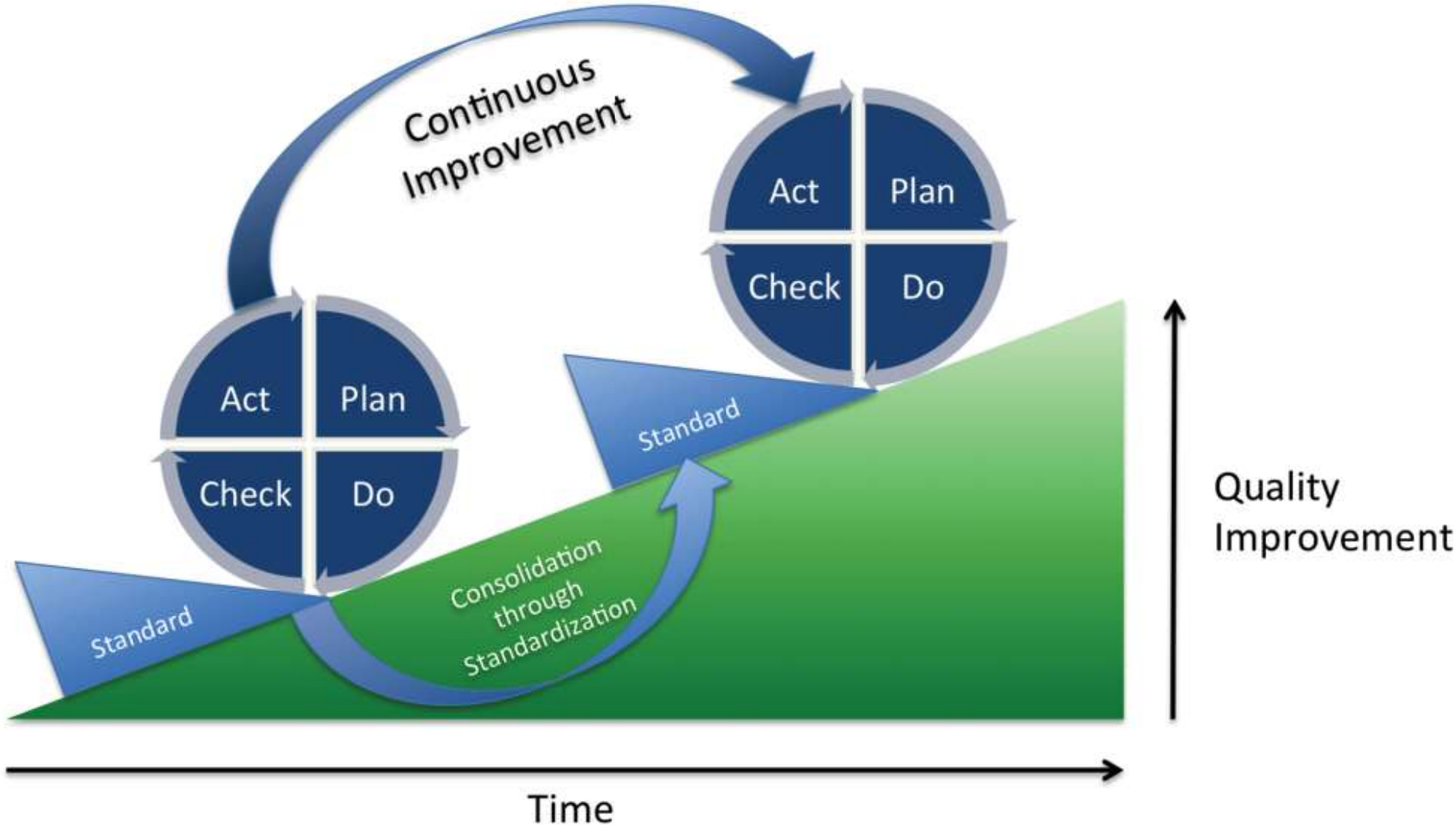
- Be thoughtful about communications regarding an incident
- Attempt to maintain Privilege

Post-Incident Report

- Collect information, perform root cause analysis, identify and investigate problems, and take appropriate and effective corrective action to prevent their recurrence actions

Corrective actions & corrections

- Address exposed vulnerabilities
- Review effectiveness of IRP


Continuous Improvement
Act
Plan
Check
Do
Act
Plan
Check
Do
Standard
Standard
Consolidation through Standardization
Quality Improvement
Time

ISO 27001 (ISMS) and 27701 (PIMS) and 42001 (AIMS)

1. Understanding and Commitment

- **Awareness:** Ensure stakeholders grasp ISO/IEC 42001's purpose and benefits.
- **Commitment**: Gain top management's commitment to implementing and maintaining an AI management system.

2. Scope Definition

- **Identify AI Activities**: Determine which AI processes, products, or services are included.
- **Exclusions**: Clearly define any excluded areas.

3. Leadership and Governance

- **Appoint a Responsible Person**: Designate someone to oversee AI management.
- **Policy Development**: Create an AI policy aligned with organizational goals.

4. Risk Assessment and Opportunity Identification

- **Assess Risks**: Identify and evaluate risks linked to AI deployment.
- **Identify Opportunities**: Spot chances to enhance AI processes.

5. AI Implementation and Operation

- **Design and Development**: Implement AI systems following established guidelines.
- **Data Management**: Ensure data quality, privacy, and security.
- **Testing and** Validation: Validate AI models and algorithms.
- **Deployment**: Roll out AI solutions in a controlled manner.

6. Monitoring and Measurement

- **Performance Metrics**: Define metrics to gauge AI performance.
- **Monitoring**: Continuously monitor AI systems for effectiveness and compliance.

7. Feedback and Improvement

- **Feedback Loop**: Set up channels to gather feedback from users, stakeholders, and employees.
- **Improvement Actions**: Regularly review and enhance AI processes based on feedback and performance data.

8. Documentation and Records

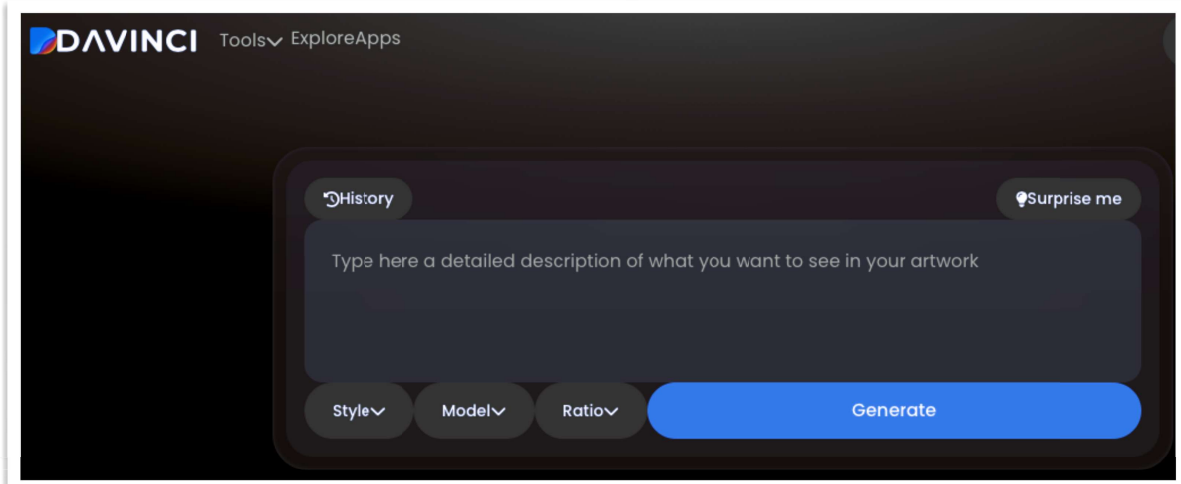
- **Document Control**: Maintain records related to AI management.
- **Training Materials**: Develop training materials for employees involved in AI activities.

9. Internal Audits and Reviews

- **Regular Audits**: Conduct internal audits to check compliance with ISO/IEC 42001.
- **Management Review**: Periodically assess the AI management system's effectiveness.

10. Continual Improvement

- **Learn and Adapt**: Continuously learn from experiences and adapt AI practices.
- **Stay Updated**: Keep abreast of AI technology advancements and best practices.



What can I help with?

Message ChatGPT

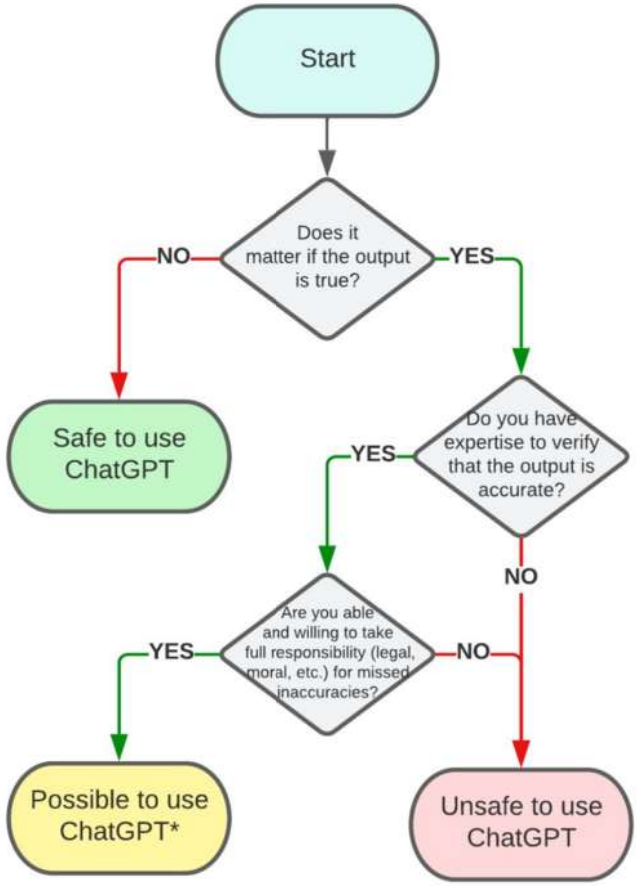
Create image | Analyze images | Summarize text | Brainstorm | More

You've hit the Free plan limit for GPT-4o.
Responses will use another model until your limit resets after 8:30 PM.

Get Plus

Is it safe to use ChatGPT for your task?

Aleksandr Tiulkanov | January 19, 2023



* but be sure to verify each output word and sentence for accuracy and common sense


Questions?

THANK YOU

Calc - you - later!

Preston Bukaty

+1 913-424-5707

pbukaty@sbcglobal.net

https://www.linkedin.com/in/preston-b-attorney-jayhawk/