State Privacy Laws and Federal Privacy Regulations: How to Operationalize Compliance

Thomas Kearney
Betsy Hodge
Christy Hawkins

November 30, 2021

akerman

1

Today's Presenters

- Thomas J. Kearney, Chair, Data Privacy and Security

- Elizabeth, "Betsy" Hodge, Partner

- Christy S. Hawkins, Special Counsel

2

Overview

- Privacy Law Developments
- Data Security Law Developments
- Latest Threats
- Strategies to Address Increasing Privacy and Security Regulations

akerman

3

U.S. Patchwork

- No comprehensive data privacy/security law
  - there are a number of sector-specific federal laws & regulations, e.g., GLBA, HIPAA
- States are enacting their own data privacy, security and breach notification laws
- At state level 3 types of laws:
  - data privacy
  - data security
  - breach notification

akerman

4

Privacy Law Developments

akerman

5

Global Privacy Laws

- **United States**
  1. California
  2. Virginia
  3. Colorado
  4. TBD 2021/2022
- **Canada**
- **Brazil**
- **China**
- **Japan**

~ Privacy Laws Are Evolving Globally ~

6

U.S. Federal Privacy Laws, Regulations, Obligations

- Gramm-Leach-Bliley Act – Regulation P (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- 42 C.F.R. Part 2 (confidentiality of substance use disorder treatment records)
- Family Educational Rights and Privacy Act (FERPA)
- FTC Privacy Rule

7

Privacy Bills in Congress

- H.R. 474 – Protecting Consumer Information Act
- H.R. 1816 – Information Transparency & Personal Data Control Act

- Challenges with passing comprehensive federal data privacy law:
  - preemption of state law
  - enforcement – private right of action?
  - existing federal sector-specific laws

8

U.S. State Laws

- California Consumer Privacy Act of 2018 ("CCPA")
- California Privacy Rights Act of 2020 ("CPRA") (effective January 1, 2023)
- Virginia Consumer Data Privacy Act ("VCDPA") (effective January 1, 2023)
- Colorado Privacy Act ("CPA") (effective July 1, 2023)

The CCPA

- How Does It Apply?
  - "Business" = for profit entity,
  - collects or directs collection of consumers' information,
  - meets revenue or information transfer thresholds
- Revenue Threshold – Revenue from California Operations, or Global?
- Key Points:
  - Transparency
  - Consumer Rights
  - Opt-Out of Sale
  - Private Right of Action

What's Next? The CPRA

- Effective Jan. 1, 2023
- Key Points:
  - "Reasonable Security" Obligation
  - New Consumer Rights:
    - Data Correction
    - Limiting Use / Disclosure of Sensitive Information
    - Automated Decision-Making
  - Extended exemptions for employee data until January 1, 2023
  - New obligations and clarifications for service providers / vendors
    - Contract requirements
    - Downstream CPRA compliance required

11

Virginia Consumer Data Protection Act

- Effective Jan. 1, 2023
- Key Points:
  - Vendor and Service Provider Relationships
    - Data Processing Agreements
  - Data Subject Rights
  - Privacy Notice
  - Technical Safeguards
  - Limits on Collection and Use
  - Principles of Data Processing
  - Data Protection Assessments

12

Colorado Privacy Act

- Effective July 1, 2023
- Key Points:
  - Vendor and Service Provider Relationships
    - Data Processing Agreements
  - Privacy Notice
  - Principles of Data Processing
  - Data Protection Assessments
  - Data Subject Rights
    - Opt Out of Targeted Advertising
    - Universal Opt Out Mechanism
  - Controller and Processor Roles and Responsibilities

13

Consumer Rights

- Right of Access
- Right of Correction
- Right of Deletion
- Right of Restriction
- Right of Portability
- Right to Opt-Out of Sale
- Right Against Automated Decision Making

14

Business Obligations

- Notice/Transparency
- Risk Assessments
- Prohibition on Discrimination (Exercising Rights)
- Purpose Limitation
- Monitor contractors

akerman

15

15

Security Law Developments

akerman

16

Security Laws, Regulations & Obligations

- NYDFS Cybersecurity Insurance Guidance
- FTC Security Rule
- PCI DSS
- HIPAA
- NAIC Insurance Data Security Model Law
- FTC Rule – Standards for Safeguarding Consumer Information
- HITECH Act Amendment – Recognition of Security Practices
- May 12, 2021 Cybersecurity Executive Order
- U.S. TSA – Emergency Directives to Critical Infrastructure Companies

akerman

17

Common Security Requirements

Administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of data

- Designate individual to oversee the organization's information security program
- Inventory the organization's data, equipment, and processes
  - How data flows through organization
- Conduct regular risk assessments to identify
  - threats and vulnerabilities,
  - likelihood of occurrence, and
  - relative harm to organization
- Develop risk management plan based on risk assessment findings
- Incorporate cybersecurity into operational processes (no silos!)

akerman

18

Data Breach Notification Laws

- All 50 states and D.C. have data breach notification laws
- 2021 Updates:
  - new notice requirements
  - broaden existing definitions (e.g., expand the definition of "personal information")
  - increase reporting content requirements
  - regulate the insurance industry
  - regulate the tax industry
  - require stricter notification timeframes
  - allow the Attorney General to publish data breach information
  - new federal bank security incident notification requirements

19

Cybersecurity for the Business

- Vendors as Personal Data Processors
- Increased Security/Privacy Protections
- Vendor Diligence is Key
- Data Breaches Caused by Vulnerability in Third-Party Software: 16%
  - Nobelium / Microsoft
- Business Responsibilities to Choose Vendors Wisely
- Example: EU GDPR, HIPAA, GLBA

20

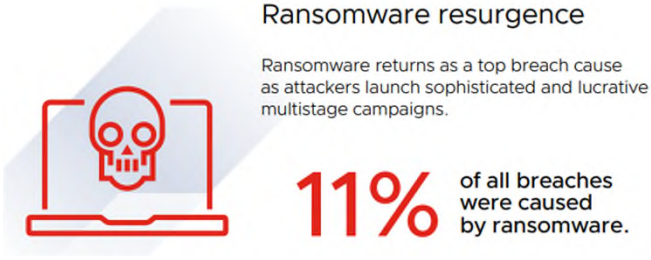
Latest Threats

akerman

21

Cybersecurity Threat Landscape

Ransomware



VMWare U.S. Security Insights Report 2021

akerman

22

Cybersecurity Threat Landscape

Ransomware

- High Profile Attacks:
  - Colonial Pipeline
  - SolarWinds

400%

CrowdStrike Holdings

23

Cybersecurity Threat Landscape

- Ransom demands and payments increasing
  - Colonial Pipeline paid $4.4 million
  - JBS USA paid $11 million
  - CNA Financial Services paid $40 million
- OFAC September 21, 2021 Advisory
  - updates 2020 Advisory on sanctions risks for companies that pay ransoms to organizations on the Specially Designated Nationals or blocked individuals list
  - all entities involved in facilitating a ransom payment to SDNs are subject to sanctions
  - payment of ransoms is strongly discouraged
  - companies should focus on improving their cyber resiliency

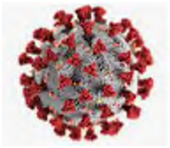
24

Cybersecurity Threat Landscape

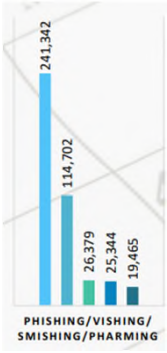
Phishing

- 14% of Security Breaches Caused by Phishing
  - *IBM 2020 Cost of a Data Breach Report*
- Attackers and Tools are More Sophisticated
- Attackers Create a Sense of Emergency or Panic
- Increased Use of Mobile Devices
  - Same Red Flags
  - More Difficult to Spot on Mobile Devices

Using COVID-19 as "Bait"



Phishing Complaints to IC3 Have DOUBLED Since 2019



IC3 Internet Crime Report 2020

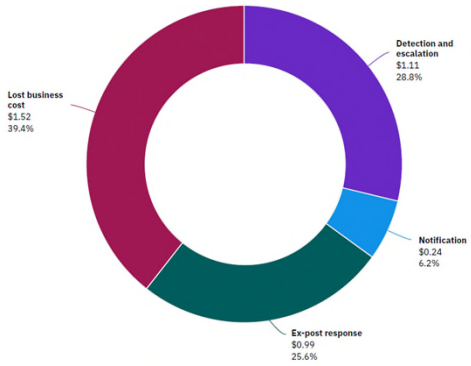
akerman

25

Cybersecurity Threat Landscape

Data Security Incidents

- Average Cost of Data Breach: $3.86 mil
  - Detection and Escalation
  - Lost Business
  - Notification
  - Ongoing Response/Mitigation
- Average Cost of $150 per record
- Average Time to Identify and Contain Data Breach: 280 Days



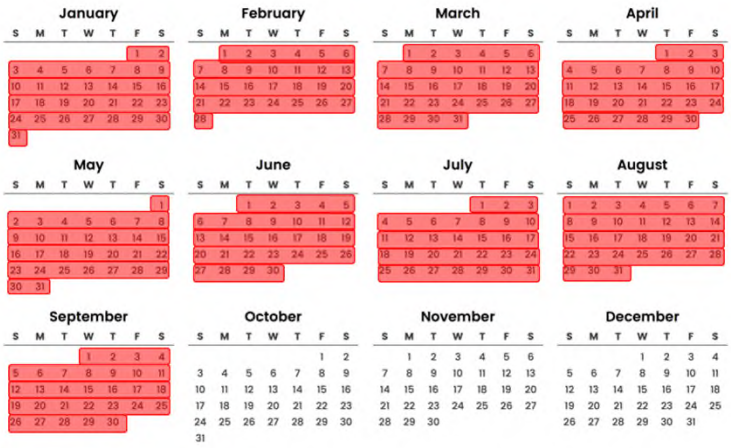
IBM 2020 Cost of a Data Breach Report

akerman

26

Cost of a Data Breach

Average Time to Identify and Contain Data Breach: 280 days

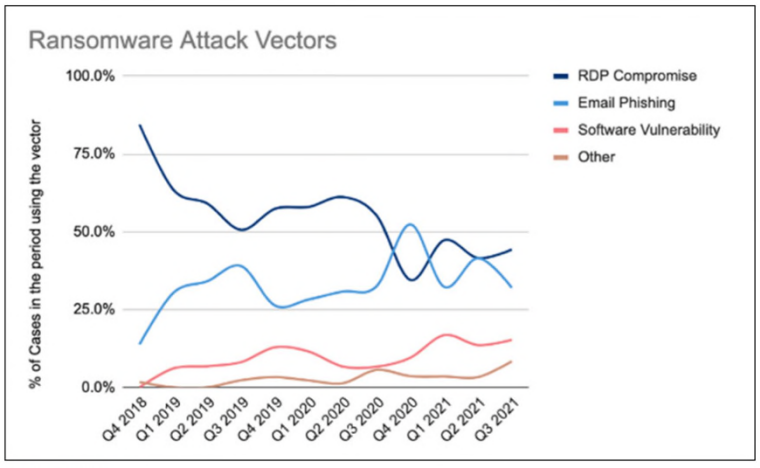


IBM Cost of a Data Breach Report, 2020

akerman

27

Cybersecurity Threat Landscape

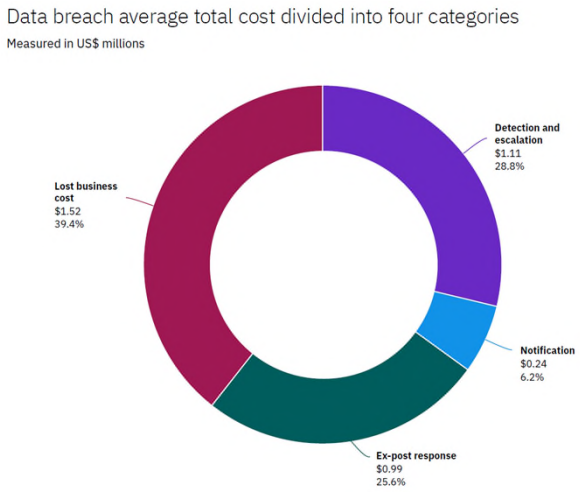


Source: Coveware

akerman

28

Cost of a Data Breach

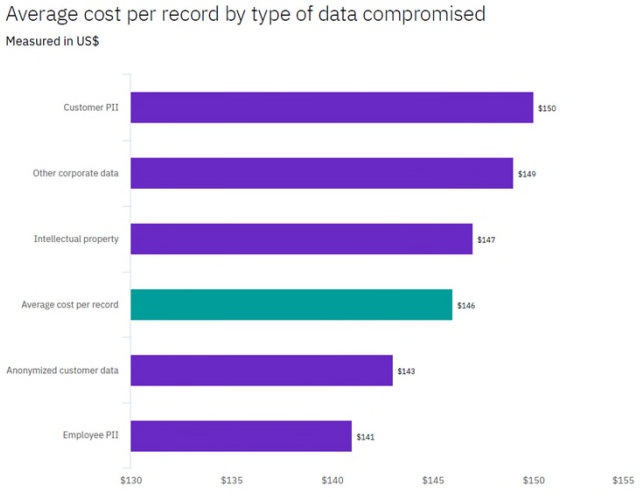


IBM Cost of a Data Breach Report, 2020

akerman

29

Cost of a Data Breach



IBM Cost of a Data Breach Report, 2020

akerman

30

Cybersecurity Threat Landscape

Cybersecurity Insurance

- Direct Written Premium for Cyber Insurance Increase:
  - 2015: $225 million
  - 2020: $1.575 billion
- NYDFS Cybersecurity Insurance Risk Framework
  - February 2021
- Cost of coverage is increasing
  - some insurers signaling they may not cover ransom payments
- Insurers conducting more underwriting of potential insureds

akerman

31

Cybersecurity Risks

Other Important Dangers/Risks

- Reputation
- Interconnectedness
- Proprietary Business Data
- Regulatory Investigations
- Legal Risks:
  - Fines
  - Consumer Lawsuits
  - Injunctions: No Longer Allowed to Collect, Use, Share Personal Data

akerman

32

Strategies for Compliance

akerman

33

Data Privacy and Security as a Business Advantage

- Accountability: Demonstrate Good Practices and Protections
- Ability to Support Privacy Rights
- Document Protections in Place
- Demonstrate Compliance with Standards
- Risk Assessments
- Data Mapping / Records of Processing
- Documented Analyses Available for Relevant Sector Clients / Business Partners

akerman

34

Strategies for Compliance

- Start with the Fundamentals:
  - Data Mapping
  - Data Retention / Deletion
- Understand How Privacy Principles Impact Your Business
- Which Laws Apply?
- Identify Common Requirements
  - Privacy Notice
  - Vendor Contracts
  - Data Subject Rights
  - Technical Safeguards
- Prioritize Based on Requirements and Risk Assessment

NY CLE Verification Code:

- For those wishing to receive New York CLE credit, please note the following code on your attendance sheet:

Code will be given during presentation

akerman

37

Akerman LLP
700+ Lawyers
24 Offices

akerman.com

akerman

38