

Cybersecurity and Privacy

A How-To-Guide

October 7, 2020



HUNTON
ANDREWS KURTH





Please note that the following is intended to be used for general guidance purposes only — it is not intended to constitute legal advice, nor is it a dispositive position on coverage. Each claim is subject to review by the applicable insurer and coverage is dependent upon the terms and conditions of your specific insurance policy.

The Privacy and Cybersecurity Team at Hunton Andrews Kurth

- Over 45 privacy and data security professionals in the U.S., EU and Asia.
- Our privacy clients have included 6 of the Fortune 10.
- We represent clients across multiple industry sectors, including technology, financial services, retail, consumer products, health care, publishing, advertising, transportation, insurance and energy.
- Centre for Information Policy Leadership at Hunton Andrews Kurth LLP

www.HuntonPrivacyBlog.com | Twitter: [@hunton_privacy](https://twitter.com/hunton_privacy)

What's the Difference Between Privacy and Data Security?

- Privacy is the appropriate use of personal information as defined by:
 - Cultural Norms/Individuals' Expectations
 - Laws and Regulations
- Security is the Protection of Information
 - Safeguards Applied to Data and Systems
 - Confidentiality
 - Data Integrity



CYBERSECURITY AND PRIVACY

U.S. Cybersecurity Law



HUNTON
ANDREWS KURTH

Cybersecurity Landscape



How are Cybersecurity Incidents Identified?

53%

of victims were notified by external entity

47%

of victims discovered breach internally

31%

of victims subsequently re-attacked within 12 months

56

Median # of days until adversary presence was discovered on victim network

Source: FireEye Mandiant Services, M-Trends 2020 Special Report, February 2020

The Cyber Threat Landscape

- **Threat Actors**
 - Organized Crime
 - Nation States
 - Hacktivists
- **Targeted Information and Systems**
 - Personal Information
 - Trade Secrets, R&D and Other Confidential Business Information
 - Critical Infrastructure
 - Cloud Environments and Source Code Repositories
- **Threat Vectors**
 - Social Engineering/Phishing
 - Credential Stuffing and Other Brute Force Attacks
 - Vendors and Insiders
- **Recent Trends**
 - Ransomware
 - Cyber Extortion
 - Business Email Compromises/Fund Diversion
 - Doxing

U.S. Data Security Rules

Federal Data Security Requirements

- Consumer Personal Information (FTC)
- Health Information (HIPAA/HITECH)
- Financial Information (Gramm-Leach-Bliley)
- Cybersecurity Risk Disclosure (SEC)
- Cybersecurity Information Sharing (CISA)

State Data Security Requirements

- Data security Laws – CA, CO, MA, NV, NY, OH, OR and Progeny
- Data Breach Notification Laws – 50 States + DC, Guam, PR and USVI
- CCPA's New Liability Scheme For Data Breaches
- Financial Institution and Insurer Regulations – e.g., NY, SC, CT, NH, NAIC
- IOT Law – CA, OR
- Biometric Data Laws – IL, TX, WA

Industry Standards

- NIST Cybersecurity Framework
- PCI DSS
- ISO 27000-Series Standards
- CIS's Top 20 Critical Security Controls

U.S. Cyber Regulatory and Legislative Trends

- U.S. data security laws continue to endorse a risk-based approach.
- At the same time, data security rules are becoming more detailed and prescriptive.
- Shifting away from principles-based laws.
- Examples – NYDFS, NH, SC, OR, MA and FTC's proposed Safeguards Rule.
- The scope of protected data is expanding.
- Broadening the definition of PI to cover online access credentials, biometric data, health information, and other elements of PI.
- Protecting more than PI such as material confidential business information and connected devices.
- Introducing safe harbors and liability protections (OH, CISA).
- Establishing accountability mechanisms such as:
 - Board Oversight and Reporting
 - Regulator Reporting Obligations

Cyber Governance: The Role of the Board

- The board sets cybersecurity tone and direction.
- Target was a wake-up call.
- Cybersecurity is a fundamental risk issue for organizations.
- Board's cyber governance duties are grounded in risk management obligations.
- Board oversight of cybersecurity program is critical to exercising fiduciary duties.
- Case law provides scant direction regarding cybersecurity oversight.
- Takeaway 1 – An extensive board-supervised cybersecurity program is sufficient to defeat a fiduciary breach claim.
- Takeaway 2 – The board must be sufficiently informed to make valid business judgments related to cybersecurity oversight.
- While cybersecurity oversight responsibilities may be delegated to a committee, the full board retains overall responsibility.
- Legal Risk to Board Members
- Shareholder actions (e.g., Marriott, Google, Yahoo, Home Depot, Wyndham, Equifax, PayPal).
- Directors Ousted

Effective Cyber Oversight

Case law and best practice principles suggest that board should:

- Understand the organization's current threat environment and crown jewels.
- Review the organization's IS governance structure to ensure appropriate oversight.
- Understand the organization's overall IS program budget and critical security initiatives.
- Oversee the organization's cybersecurity risk management and audit functions.
- Hold management accountable by reviewing the organization's key cybersecurity strategies and preparedness efforts.
- Receive benchmarking reports on how security practices compare to industry peers.
- Stay informed about the organization's significant cybersecurity incidents, including updates on incident costs and potential consequences.
- Ensure appropriate outside experts are identified in advance of an incident.
- Consult outside experts to gain independent perspective on cyber risks.
- Ensure the board's cybersecurity oversight responsibilities and activities are appropriately documented (e.g., in charters, meeting minutes, policies).

Proactive Measures: Preparing for the Worst

- Identify and Classify Sensitive Data
- Ensure Written Information Security Policies are State-of-the-Art
- Test and Patch Your Software and Systems
- Continually Audit and Assess the Status of Security Measures
- Maintain Incident Response Plan.
- Prepare Data Breach Toolkit
- Prepare Incident Response Team Through Tabletop Exercises
- Manage Vendor, Employee and Supplier Risks
- Assess Cybersecurity Risk in M&A Transactions
- Train Employees and Increase Cybersecurity Awareness
- Evaluate Cyber Insurance Needs

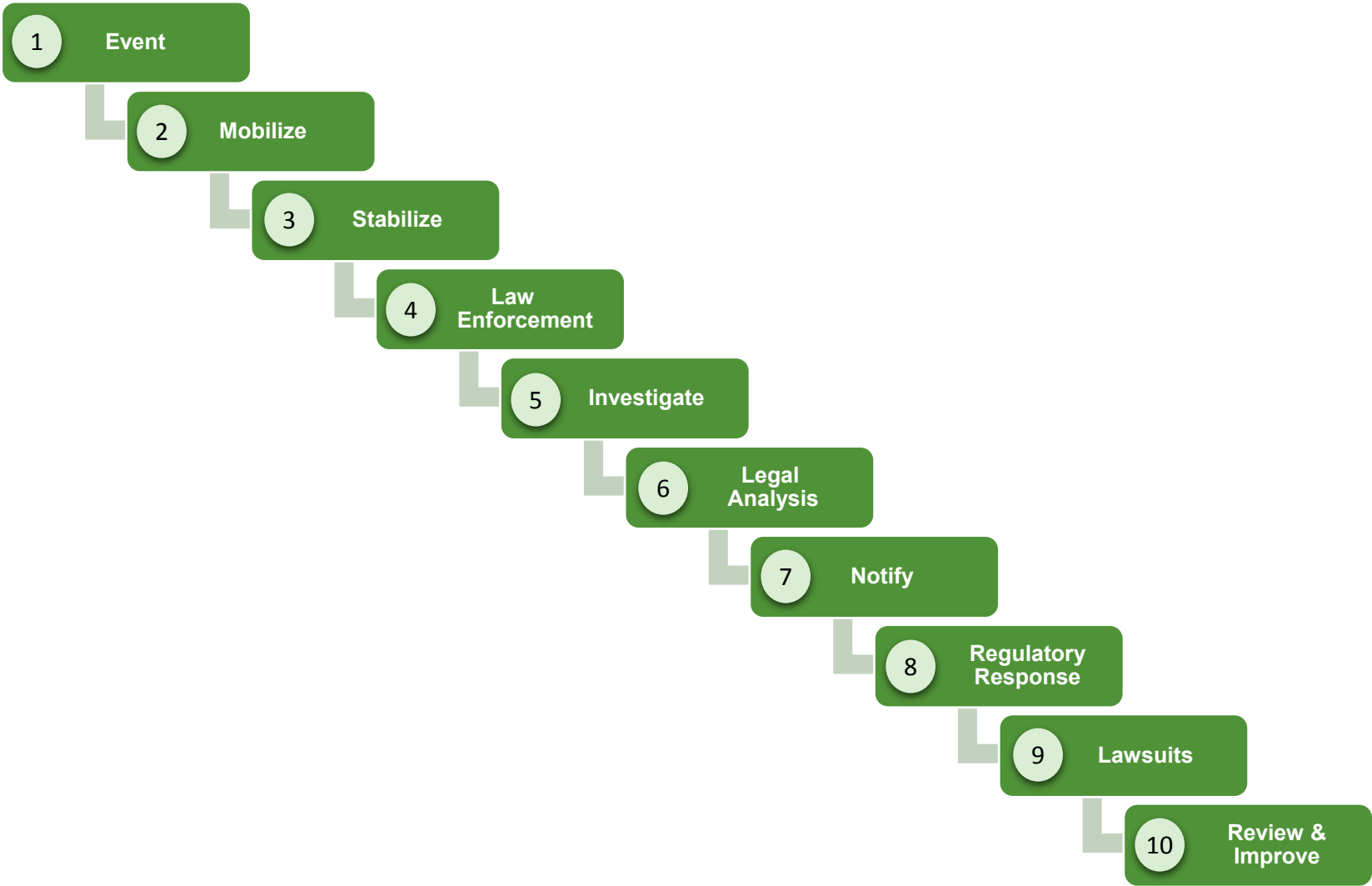
CYBERSECURITY AND PRIVACY

Legal Issues in a Cyber Attack



HUNTON
ANDREWS KURTH

Cybersecurity Incident Response Timeline




Incident Liability and Ramifications

- Regulatory Enforcement
- Congressional Inquiries
- Payment Card Fines and Assessments
- Civil Litigation
- Reputational Damage
- Financial Loss Arising Directly From the Criminal Conduct
- Response and Recovery Expenses
 - Investigation and Notification Costs
 - Remediation and Improvement Costs
- Turnover
 - CEOs and C-Suite Executives Blamed
 - Board Members Threatened With Ouster

Lessons Learned: Breach Response Protocols Are Changing

- Criminals are Far More Sophisticated
 - Detection is More Difficult
- Timing of Notification has Changed
 - Need to quickly convene incident response team and conduct forensic investigation upon learning of a potential security issue.
 - Cannot bury one's head in the sand when investigating.
- Social Media Forces the Hand of PR Strategy
- Credit monitoring is essentially mandatory for data compromises where monitoring is not useful (e.g., credit cards).
- Individuals are more sensitized to cybersecurity events.
 - Pros and Con
- Focus on Cybersecurity Must Come From the Top
 - Senior leadership must provide strategic cyber direction and guidance.



CYBERSECURITY AND PRIVACY

U.S. Privacy Law



HUNTON
ANDREWS KURTH

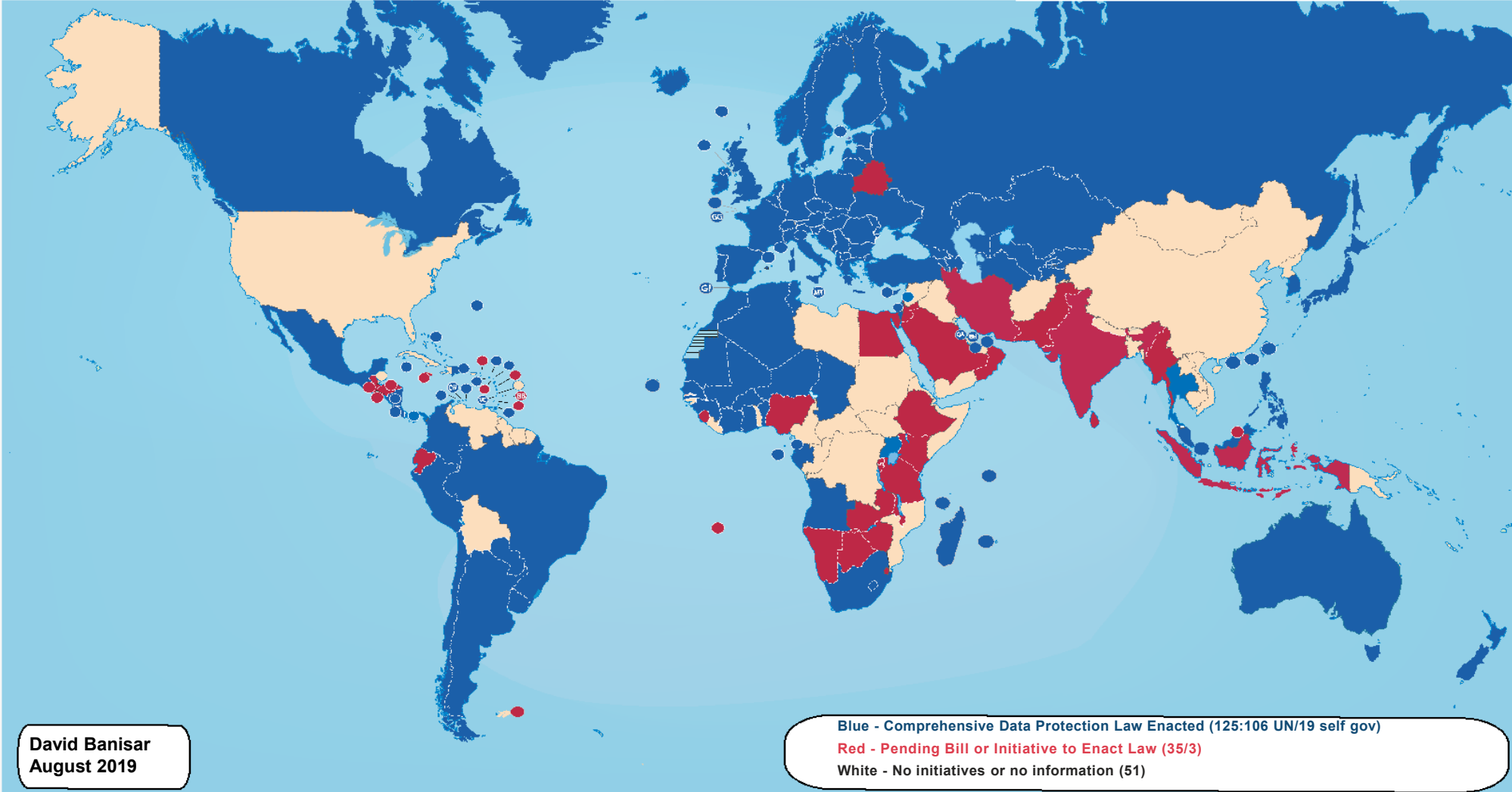
Why is Privacy Important?

- Data is the New Oil
- Four Privacy Risks
 - Legal Compliance
 - Reputation
 - Investment
 - Retention
- Privacy by Design
 - Cacophony of Laws Mandates this Concept
 - Businesses Should Promote Consumer Privacy Throughout the Organization and at Every Stage
 - Trust is Everything
- New Focus on Data Ethics and Discrimination

Global Data Protection Landscape

- Living in the information age.
- Legislators and regulators around the globe are grappling with vexing policy issues.
 - Laws exist or are under serious consideration in nearly every industrialized nation.
- Some legal regimes are relatively new, while others are more mature.
 - Government enforcement has increased dramatically.
- Approach to data protection is highly dependent on a country's historical and cultural experience.
- Understanding the data privacy and security landscape is a key strategic consideration for global companies.

National Comprehensive Data Protection/Privacy Laws and Bills 2019



Major U.S. Federal Privacy Laws

Sectoral Federal Approach in the U.S., Including:

- FTC Act – Consumer Protection
- HIPAA – Health Care Entities and Business Associates
- GLB – Financial Institutions
- Fair Credit Reporting Act (FCRA/FACTA/FTC Disposal Rule) – Consumer Reporting Agencies and Others
- CAN-SPAM – Commercial Email
- Video Privacy Protection Act – Video Rental Records
- Driver's Privacy Protection Act – DMV Records
- Telephone Consumer Protection Act – Telemarketing
- Children's Online Privacy Protection Act – Children's Data Collected Online
- Privacy Act of 1974 – Federal Government

State Privacy Laws

Hundreds of State Privacy Laws, Including

- California Consumer Privacy Act of 2018
- Health Privacy Laws
- Biometric Privacy Laws
- Website Privacy Notices
- SSN Use Restrictions
- Marketing Restrictions (E.G., Telemarketing)
- Restrictions on Third-party Information Sharing For Marketing Purposes
- Child Protection Registry Laws
- Financial Privacy Laws
- Radio Frequency Identification
- Anti-spyware
- Credit Reports
- Privacy Torts
- Data Brokers
- Broadband Providers

CCPA Changed the U.S. Privacy Landscape

- The CCPA changed the privacy landscape in the U.S.
 - First General U.S. Privacy Law
- Grants California “consumers” certain rights over their personal information.
 - Right to Access
 - Right to Delete
 - Right to Opt Out of Sale
- Requires businesses subject to the law to disclose specified, detailed content in the business’s privacy policies.
- Requires businesses to contractually restrict the activities of service providers that process personal information.
- Mandates specific CCPA training of relevant personnel.
- Compliance Deadline – January 1, 2020
- Enforcement Date – July 1, 2020
- Enforceable by CA AG and limited private right of action in connection with certain data breaches.
 - Statutory damages of up to \$750 per consumer per incident or actual damages.

Uptick in Enforcement

Government Enforcement has Increased Significantly

The stakes have never been higher:

- Facebook – \$5 Billion FTC Settlement and \$100 Million SEC Settlement (July 2019)
 - Also, \$550 million BIPA consumer class action settlement (January 2020).
- Equifax – \$700 Million Settlement With FTC and 48 States (July 2019)
- British Airway – \$230 Million Fine by the UK ICO (July 2019)
- Marriott – \$124 Million Fine by the UK ICO (July 2019)
- Yahoo – \$117.5 Million Consumer Class Action Settlement (June 2019)
- Google – \$57 Million Fine by the French CNIL (January 2019)
- Uber – \$148 Million Settlement With All 50 States (September 2019)
- Capital One – \$80 Million Settlement With OCC (August 2020)

More is on the Horizon – e.g., High CCPA Statutory Penalties

Global Convergence: Operationalizing Privacy Going Forward

- Global cacophony demands a high-level approach to privacy compliance.
- Organizations with mature privacy functions will establish a single global program, with tweaks to comply with local legal vagaries.
- Meaningful and consumer-first privacy approaches will be most effective.

Thank You

Primary Point of Contact:

Lisa J. Sotto

lsotto@hunton.com

212.309.1223

www.HuntonPrivacyBlog.com

 [@Hunton_Privacy](https://twitter.com/Hunton_Privacy)

www.Hunton.com



HUNTON
ANDREWS KURTH