Cybersecurity Legal Framework: Federal and State Requirement

By Craig Besnoy

Craig Besnoy is a Partner at Dunlap Bennett & Ludwig, where he advises on cybersecurity, data privacy, and regulatory compliance with a core focus on mergers, acquisitions, and strategic transactions involving data-driven and highly regulated businesses. He works extensively with healthcare organizations, financial services firms, technology companies, and investors on cybersecurity risk management, HIPAA compliance, incident response, and third-party risk oversight.

Craig has more than a decade of experience advising on complex transactions and compliance matters in which data security and privacy risk are material considerations, including acquisitions, restructurings, and growth-stage investments. His experience includes helping physician-owned practices achieve HIPAA compliance and training physicians and staff on privacy and security best practices as part of pre-acquisition readiness efforts. He is admitted to practice in New York and is recognized for translating evolving cybersecurity and privacy regulations into operationally practical and legally defensible frameworks.

DUNLAP BENNETT & LUDWIG

This guide is provided for general informational purposes only and does not constitute legal advice. It does not create an attorney-client relationship. Cybersecurity obligations vary based on industry, jurisdiction, data types, and risk profile. Organizations should consult counsel regarding their specific regulatory and contractual obligations

Understanding Cybersecurity Laws in the United States

Federal rules set the floor, sector standards raise it, and state laws fill gaps. Most organizations operate under layered obligations: a risk-based security program, vendor oversight, breach readiness, and incident reporting when thresholds are met. NIST guidance anchors most programs, agency rules shape enforcement, and documentation supports defensibility.

For teams mapping cybersecurity obligations, this guide offers plain-language context and cites primary rules that drive action. Leaders under pressure find fast framing here. Counsel mapping multi-jurisdictional duties find practical checkpoints. The sections connect statutes to day-to-day controls, touch cyber insurance alignment, and clarify how federal, sector, and state layers interact.

Who This Guide Is Designed For

This guide is designed for in-house legal teams, CISOs, compliance leaders, board members, and executives responsible for overseeing cybersecurity risk. It is also relevant for organizations preparing for M&A transactions, regulatory examinations, cyber-insurance renewals, or incident response planning. The focus is on translating legal requirements into operational guardrails that can be documented, tested, and defended.

How the US Cybersecurity Legal System Works

The United States does not codify cybersecurity in one statute. Organizations navigate a layered system. Congress sets baseline statutes. Federal agencies publish rules and bring enforcement cases. Sector regulators add control-specific expectations. States pass privacy and breach notification laws. International partners set cross-border duties when data flows abroad.

- **Federal baseline.** Core laws like the Computer Fraud and Abuse Act govern unauthorized access and criminal conduct. Other statutes shape privacy and information sharing.
- **Agency enforcement.** The FTC uses unfairness authority for inadequate security. DOJ brings criminal cases and partners with the FBI. CISA coordinates national defense and shares advisories.
- **Sector overlays.** HIPAA for health data, GLBA for financial institutions, and NERC CIP for bulk electric system owners.
- **State rules.** All 50 states have breach notification laws. California and others add privacy and security duties.

Program guidance centers on NIST. As of 2025, NIST Cybersecurity Framework 2.0 is the dominant reference. While NIST frameworks are voluntary, regulators and courts routinely treat them as evidence of reasonable security practices, making documented alignment critical for enforcement defense and breach litigation. Federal agencies use FISMA for federal systems and require risk management, continuous monitoring, and incident response plans tied to NIST standards.

Federal Cybersecurity Statutes and Governance

Congress sets the legal foundation through statutes, then the Executive Branch implements through orders, guidance, and budget controls. The Federal Information Security Modernization Act directs how civilian agencies manage risk across information systems and assigns OMB and DHS oversight for metrics and incident reporting on federal networks. The White House has directed software supply chain improvements, zero-trust strategies, and event reporting through executive actions following major incidents.

NIST builds voluntary frameworks and standards used by government and industry. NIST Cybersecurity Framework 2.0, released in 2024, expanded governance and supply-chain guidance and remains the most cited model for program alignment and third-party risk oversight. CISA leads national coordination, shares advisories through Shields Up, partners through the Joint Cyber Defense Collaborative, and provides free cyber hygiene scanning for internet-facing assets.

The 2015 Cybersecurity Act created a structure for sharing cyber threat indicators and defensive measures with liability protections when procedures are followed. This supports community defense while addressing privacy concerns.

Core Federal Statutes That Shape Cybersecurity Obligations

Law	Purpose	Who it covers	Key legal risk
Computer Fraud and Abuse Act	Prohibits unauthorized access and related fraud	Any person who accesses protected computers	Criminal charges, civil claims, forfeiture
Electronic Communications Privacy Act	Protects electronic communications in transit and storage	Service providers, law enforcement, private actors	Criminal penalties, civil suits, suppression risk
Cybersecurity Act of 2015	Information sharing with liability protections	Private and public entities that share indicators	Compliance with sharing procedures and privacy limits

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act at 18 U.S.C. § 1030 is the main federal anti-hacking law. It covers unauthorized access, exceeding authorized access, password trafficking, and damage to protected computers —systems used in or affecting interstate or foreign commerce. It supports both criminal prosecutions and civil lawsuits. DOJ charging policies guide cases toward malicious conduct and away from chilling security research.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act is a bundle of rules. The Wiretap Act covers interception of communications in transit. The Stored Communications Act covers access to communications in storage. The Pen Register statute covers dialing and routing information. These rules shape logging, monitoring, and law enforcement process for email, messaging services, and cloud platforms. Companies commonly document lawful basis for monitoring and adopt clear banners and consent where required.

Cybersecurity Information Sharing Act

The Cybersecurity Act of 2015 includes the Cybersecurity Information Sharing Act title. It encourages sharing of cyber threat indicators and defensive measures with CISA and among private parties. It grants targeted liability protections for sharing in accordance with the statute, includes privacy guidelines, and directs removal of personal information not directly related to the cyber threat. Companies that participate commonly operationalize scrubbing, use approved channels, and maintain records of what was shared and why.

Agency Enforcement and Guidance Patterns

Federal Trade Commission unfair practices enforcement

The FTC has repeatedly found that materially inadequate data security practices may constitute an unfair practice under Section 5 of the FTC Act, particularly where organizations fail to implement controls they publicly represent or that are widely accepted as baseline safeguards.. Cases have focused on weak access controls, lack of encryption for sensitive data, poor vulnerability management, and failure to follow stated policies. The FTC Safeguards Rule under GLBA adds specific requirements for financial institutions, with recent amendments expanding risk assessments, multifactor authentication, and reporting for certain events. Consent orders typically mandate program upgrades and outside assessments.

Department of Justice and FBI cyber crime actions

DOJ and the FBI bring cases under the CFAA, wire fraud, identity theft, and money laundering. Recent takedowns have targeted botnets, ransomware affiliates, and crypto laundering networks. The FBI Internet Crime Complaint Center collects victim reports to support investigations and recovery activity. Early engagement with law enforcement can support decryption keys and asset tracing in some events.

Cybersecurity and Infrastructure Security Agency programs

CISA publishes alerts on vulnerabilities and exploits, including Known Exploited Vulnerabilities catalogs that agencies must address and that industry can adopt by policy. Shields Up advisories raise posture during heightened threat periods. CISA also operates vulnerability scanning, phishing assessment, and incident response support on request. Engagement with the Joint Cyber Defense Collaborative can accelerate sharing with peers and government.

Sector-Specific Cybersecurity Obligations

Healthcare security and HIPAA requirements

Covered entities and business associates must implement administrative, physical, and technical safeguards under the HIPAA Security Rule. Risk analysis, access controls, audit trails, integrity, and transmission security are required elements. The Breach Notification Rule sets a low probability of compromise standard and timelines for notice to individuals and HHS when unsecured protected health information is exposed.

Financial services and GLBA safeguards

Financial institutions under GLBA must maintain a written information security program. The updated FTC Safeguards Rule adds board reporting, asset inventories, encryption at rest and in transit, multifactor authentication, secure software development practices, and written incident response plans. It also requires oversight of service providers and event reporting to the FTC in specific circumstances. Banking regulators also use the FFIEC IT Handbook and incident notification rules for banks and service providers.

Energy and critical infrastructure standards

Owners and operators of the bulk electric system under NERC jurisdiction must follow the Critical Infrastructure Protection standards. CIP covers security management controls, personnel risk assessments, electronic and physical perimeters, system security management, and incident reporting. Enforcement involves audits and penalties for noncompliance. FERC approves and directs updates to CIP when risk changes.

State Cybersecurity and Privacy Regimes

California privacy and security requirements

California's CCPA as amended by the CPRA sets consumer rights for access, deletion, correction, and opt-out of certain data sharing. It also requires reasonable security practices and regulated assessments for high-risk processing under agency rules. Separate California Civil Code sections require businesses to protect personal information with reasonable security and to notify residents of breaches without unreasonable delay.

New York Department of Financial Services rules

NYDFS Cybersecurity Regulation 23 NYCRR Part 500 applies to covered financial institutions licensed by DFS. It requires a risk-based program, CISO leadership, access controls, encryption, monitoring, vulnerability management, incident response, business continuity, and board or senior officer certification. 2023 amendments added new classes of covered entities, event notification updates, and stricter governance and testing expectations.

Other state laws and harmonization trends

All states and territories have breach notification laws. Many states now have privacy laws that look similar in structure to California's model but differ in scope and rights. Harmonization trends include risk assessments for high-risk processing, vendor contract clauses, opt-out rights for targeted advertising, and reasonable security duties. Companies commonly maintain a state law matrix and map triggers to their incident response plan.

Data Breach Notification Requirements

When notification triggers

Most state breach laws trigger when personal information is acquired or reasonably believed to be acquired by an unauthorized person. Some laws use a risk-of-harm standard. HIPAA uses a low probability of compromise standard for unsecured protected health information. NYDFS and GLBA Safeguards have separate triggers for covered institutions.

Who receives notice and timelines

Typical notifications include affected individuals, state attorneys general or consumer protection agencies for larger events, and in some states consumer reporting agencies when thresholds are met. Timelines vary by state, with many requiring notification without unreasonable delay and some setting fixed periods like 30 or 45 days. Sector rules may have shorter clocks. Documentation of timing and decision-making demonstrates good faith.

Safe harbor and encryption considerations

Many state laws include safe harbor when data was encrypted and the key was not accessed. Some laws recognize redaction or hashing in line with state definitions. HIPAA treats properly encrypted PHI according to HHS guidance as secured, which avoids breach notification. Encryption key management programs and access logs support safe harbor claims.

Cyber Incident Reporting Rules and Trends

Critical infrastructure reporting developments

The Cyber Incident Reporting for Critical Infrastructure Act requires covered entities to report covered cyber incidents to CISA within 72 hours and ransom payments within 24 hours once the final rule takes effect. CISA is conducting rulemaking to define covered entities, covered incidents, and reporting content. Organizations in critical sectors commonly plan to capture the necessary fields and update playbooks now.

Transportation and pipeline security directives

Following major incidents against pipelines, TSA issued security directives for pipeline owners and operators. These directives require incident reporting to CISA, cybersecurity assessments, implementation of mitigation measures, architecture reviews, and testing. Updates have moved to performance-based requirements and regular plan validation cycles. Similar directives have been used in rail and aviation contexts when needed.

Public company disclosure expectations

The SEC adopted rules in 2023 requiring public companies to disclose material cybersecurity incidents on Form 8-K within four business days of determining materiality, with narrow delays for national security. Annual reports must describe risk management, strategy, and governance related to cyber risk. Companies commonly develop materiality playbooks, board reporting processes, and coordination between security, legal, and investor relations.

Cyber Insurance and Legal Risk Alignment

How cyber insurance interacts with compliance

Underwriters now evaluate control maturity during placement and renewal. Core controls include multifactor authentication, privileged access management, endpoint detection and response, logging and retention, backup immutability, and vendor risk management. Better maturity can improve coverage terms and pricing. Policies often require ongoing compliance with stated controls and warranties, which ties coverage to program posture. Regulators also look for these controls.

How cyber insurance interacts with compliance

Underwriters now evaluate control maturity during placement and renewal. Core controls include multifactor authentication, privileged access management, endpoint detection and response, logging and retention, backup immutability, and vendor risk management. Better maturity can improve coverage terms and pricing. Policies often require ongoing compliance with stated controls and warranties, which ties coverage to program posture. Regulators also look for these controls.

Common exclusions and policy conditions

Policies often exclude acts of war or hostile acts, prior known incidents, intentional acts, and failure to maintain minimum security standards. Some policies limit coverage for regulatory fines where uninsurable by law. Many require prompt notice, cooperation in defense, and consent before paying ransom. Endorsements that add clarity to war and nation-state issues are common, as are sublimits for business interruption and dependent outages.

Patterns observed in coverage and control alignment

- A single source of truth for controls listed in applications and binders reduces disputes.
- Tabletop exercises that include claims notice steps and panel counsel accelerate response.
- Vendor maps tied to dependent business interruption limits and endorsements clarify coverage scope.
- Backups stored offline or logically isolated, with tested restores, improve both coverage and resilience.
- Metrics that both regulators and insurers accept, like NIST CSF outcomes, streamline audits and renewals.

Compliance Roadmap Elements

Map data systems and legal obligations

Organizations commonly start by inventorying systems and data flows, then label data types to legal regimes. The outcome is a clear map tied to HIPAA, GLBA, CCPA, and contract duties. Identifying roles such as controller or processor and financial institution status clarifies scope for rules and vendor clauses. Recording cross-border transfers and government cloud use supports planning for contractual and international risk controls.

Implement risk-based controls and testing

Enterprise risk assessments aligned to NIST CSF 2.0 commonly result in prioritized control gaps and owners. Deploying core controls like MFA, EDR, logging, vulnerability management, and encryption reduces likelihood and impact and strengthens standing with regulators and insurers. Regular testing through scanning, red and purple team exercises, and tabletop drills provides evidence of due care and accelerates response.

Prepare incident response and vendor oversight

Incident response plans that integrate legal, privacy, IT, and communications enable faster triage and accurate notifications. Law enforcement and regulator contact lists support timely reporting for CIRCIA, SEC, and sector rules. Service provider oversight with contract clauses, assessments, and monitoring builds resilience against third-party incidents and aligns with Safeguards Rule expectations.

Emerging Legislation and Policy Insights

Federal proposals that may change obligations

Final CIRCIA reporting rules are expected to set detailed definitions, deadlines, and formats for critical infrastructure. Agencies continue to propose sector-specific incident reporting harmonization to reduce duplication across SEC, banking, and state rules. Congress has also directed studies of mobile network security through the Understanding Cybersecurity of Mobile Networks Act, which may drive new guidance for cellular and 5G providers.

State-level trends

States are moving toward baseline security requirements for sensitive data, privacy impact assessments for high-risk processing, and cybersecurity governance expectations for boards in regulated sectors. More states are adopting California-style privacy statutes with unique definitions and exemptions. Updates to ransomware payment reporting and state critical infrastructure rules that mirror federal direction are emerging.

International developments that affect US firms

US companies that process European personal data must track EU GDPR transfer rules and standard contractual clauses. Global software suppliers are being asked for software bill of materials and secure development attestations by large buyers. NIST CSF 2.0 alignment helps map to many international frameworks and supports audit readiness for cross-border clients.

Patterns Observed in Durable Cybersecurity Programs

- A living inventory of systems, data types, and vendors anchors program alignment to NIST CSF 2.0 and sector rules.
- Breach notification readiness tied to legal thresholds and fast paths for incident reporting to regulators reduces timeline risk.
- Controls that insurers require, documented accurately, align coverage with operational posture.
- In M&A transactions, these same controls are increasingly evaluated as value drivers or value detractors, with unresolved cybersecurity gaps leading to purchase price adjustments, escrow holdbacks, or enhanced indemnities.

Methodology. This guide compiles primary legal texts, regulator guidance, and government frameworks. Sources include US Code, CFR, regulator sites, NIST publications, and agency press materials. Legal environments change, so confirm against current primary sources before final decisions.

Planning considerations. Quarterly refreshes of legal obligation matrices keep pace with rulemaking. Testing materiality and notification playbooks with counsel identifies gaps before events. Tracking CIRCIA rulemaking and SEC guidance supports readiness. NIST CSF 2.0 serves as a north star for mapping obligations and iterating with evidence.

Transaction Snapshot: Cybersecurity as Legal and Deal Risk

Craig Besnoy's work sits at the intersection of cybersecurity, regulatory compliance, and corporate transactions. He regularly advises companies, boards, and investors on how cybersecurity posture, data-privacy controls, and incident readiness impact valuation, deal structure, and post-closing liability. His matters frequently involve cybersecurity diligence in M&A transactions, remediation planning tied to regulatory frameworks such as NIST, HIPAA, GLBA, and NYDFS Part 500, and alignment of security controls with representations, warranties, and insurance requirements.

In addition to transaction support, Craig advises on breach preparedness and response, vendor and cloud-service governance, and regulatory exposure following security incidents. His approach emphasizes building defensible programs that can withstand regulatory scrutiny, insurance underwriting, and diligence review—focusing on documentation, risk prioritization, and governance rather than theoretical compliance.

About the Author

Craig Besnoy is a Partner at Dunlap Bennett & Ludwig, where he focuses on cybersecurity, data privacy, and regulatory compliance, with a particular emphasis on M&A and other complex transactions involving data-driven and highly regulated businesses. He advises healthcare organizations, financial services firms, technology companies, and investors on cybersecurity risk management, HIPAA compliance, incident response, and vendor oversight.

Craig has over a decade of experience advising on transactions and compliance matters where data security and privacy risk are material considerations, including acquisitions, restructurings, and strategic investments. He is admitted to practice in New York and is recognized for helping clients translate evolving cybersecurity and privacy regulations into operationally practical and legally defensible programs.

Strategic Partnership for Legal Protection

Dunlap Bennett & Ludwig advises organizations on cybersecurity governance, incident readiness, vendor risk, and regulatory compliance across federal, state, and sector-specific regimes. Our work focuses on making cybersecurity programs defensible under regulatory scrutiny, insurance underwriting, and transactional due diligence, before an incident forces the issue.

To learn more about Dunlap Bennett & Ludwig, call **888-306-4030** or email **clientservices@dbllawyers.com**.

Please note: *This article is for informational purposes only and does not constitute legal advice. The legal process is complex and highly dependent on the specific facts of your case. For guidance on your unique situation, we invite you to schedule a confidential consultation with our experienced legal team.*

References

1. 18 U.S.C. § 1030. Computer Fraud and Abuse Act. Legal Information Institute. law.cornell.edu/uscode/text/18/1030. Accessed October 21, 2025.
2. Electronic Communications Privacy Act overview. U.S. Department of Justice, CCIPS. justice.gov/criminal-ccips/electronic-communications-privacy-act. Accessed October 21, 2025.
3. Cybersecurity Act of 2015 overview. Cybersecurity and Infrastructure Security Agency. cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015. Accessed October 21, 2025.
4. Federal Information Security Modernization Act. 44 U.S.C. § 3551 et seq. law.cornell.edu/uscode/text/44/chapter-35/subchapter-II. Accessed October 21, 2025.
5. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. nist.gov/cyberframework. Accessed October 21, 2025.
6. Executive Order 14028. Improving the Nation's Cybersecurity. The White House. whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity. Accessed October 21, 2025.
7. Federal Trade Commission. Data security guidance and enforcement. ftc.gov/business-guidance/privacy-security/data-security. Accessed October 21, 2025.
8. FBI Internet Crime Complaint Center. Federal Bureau of Investigation. ic3.gov. Accessed October 21, 2025.
9. Shields Up. Cybersecurity and Infrastructure Security Agency. cisa.gov/shields-up. Accessed October 21, 2025.
10. HIPAA Security Rule and Breach Notification Rule. U.S. Department of Health and Human Services. hhs.gov/hipaa/for-professionals/security and hhs.gov/hipaa/for-professionals/breach-notification. Accessed October 21, 2025.
11. Standards for Safeguarding Customer Information. 16 CFR Part 314. Federal Trade Commission. ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314. Accessed October 21, 2025.
12. NERC Critical Infrastructure Protection standards. North American Electric Reliability Corporation. nerc.com/pa/Stand/Pages/CIPStandards.aspx. Accessed October 21, 2025.
13. California Consumer Privacy Act and CPRA. California Civil Code § 1798.100 et seq. California Privacy Protection Agency. cppa.ca.gov. Accessed October 21, 2025.
14. California Data Security and Breach Notification. Cal. Civ. Code §§ 1798.81.5, 1798.82. State of California Department of Justice. oag.ca.gov/privacy/databreach. Accessed October 21, 2025.
15. 23 NYCRR Part 500. Cybersecurity Requirements for Financial Services Companies. New York State Department of Financial Services. dfs.ny.gov/industry_guidance/cybersecurity. Accessed October 21, 2025.
16. Security Breach Notification Laws. National Conference of State Legislatures. ncsl.org/technology-and-communication/security-breach-notification-laws. Accessed October 21, 2025.
17. Cyber Incident Reporting for Critical Infrastructure Act of 2022. CISA fact sheet. cisa.gov/circia. Accessed October 21, 2025.
18. Transportation Security Administration. Pipeline cybersecurity security directives. tsa.gov/for-industry/pipeline-security. Accessed October 21, 2025.
19. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Securities and Exchange Commission Release Nos. 33-11216, 34-97989. sec.gov/rules/final/2023/33-11216.pdf. Accessed October 21, 2025.
20. National Association of Insurance Commissioners. Cyber insurance and data security resource center. content.naic.org/cipr-topics/cyber-insurance-and-data-security. Accessed October 21, 2025.
21. Lloyd's Market Bulletin Y5381. Cyber war and cyber operation exclusions. Lloyd's. lloyds.com/~/media/files/the-market/communications/market-bulletins/2022/11/y5381.pdf. Accessed October 21, 2025.