Morgan Lewis

REPORT

CYBERSECURITY & PRIVACY 2026

ENFORCEMENT & REGULATORY TRENDS

www.morganlewis.com

Morgan Lewis

CYBERSECURITY & PRIVACY 2026: ENFORCEMENT & REGULATORY TRENDS

Privacy and cybersecurity developments in 2025 were driven by ongoing regulatory development and enforcement. In the United States, federal and state authorities advanced detailed security, audit, and reporting frameworks. Across the United Kingdom, European Union, and Middle East, resilience and data governance remained core priorities, while China and other Asia-Pacific jurisdictions expanded incident reporting, cross-border transfer controls, and operational requirements.

This report highlights the most consequential regulatory, enforcement, and market trends across key geographies and offers a forward look to 2026:

- **US federal cybersecurity rules and standards advanced significantly.**
  The Cybersecurity Maturity Model Certification and DOJ's Data Security Program, which focuses on transfers of sensitive personal or government-related data to countries of concern, drove enforcement risk and national security controls across the government contracting and data ecosystems.

- **US states expanded privacy and ADMT governance.**
  California's final regulations for automated decision-making technology, cyber audits, and privacy risk assessments signaled stronger state oversight and mounting compliance burden for many companies.

- **UK/EU cybersecurity and resilience frameworks continued to mature.**
  Critical infrastructure and operational resilience requirements evolved alongside global discussions on AI governance and digital markets.

- **Middle East risk and compliance considerations deepened around infrastructure and data flows.**
  Cybersecurity expectations increasingly touched energy, infrastructure, and cloud operations, with multinational implications.

- **China established new reporting and outbound data transfer obligations.**
  Incident reporting rules and certification-based cross-border frameworks elevated scrutiny and contractual governance requirements.

- **Asia-Pacific markets pursued broader data protection and transfer alignment.**
  Regional legislative and operational changes reflected shared priorities around resilience, vendor oversight, and breach escalation.

UNITED STATES

A New Federal Playbook for Cyber Risk

CMMC Final Rule

The US Department of Defense's final Cybersecurity Maturity Model Certification (CMMC) rule of November 2025 marked a significant shift in federal cybercompliance by formally tying contract eligibility to demonstrated cybersecurity maturity across three levels aligned to the sensitivity of federal contract information and controlled unclassified information. The rule's audit and certification requirements extend through the defense industrial base via contractual flowdowns, increasing exposure for subcontractors and suppliers.

Inaccurate certifications or representations regarding cybersecurity posture now carry heightened risk under the False Claims Act even where no cyberincident has occurred, placing renewed emphasis on documentation, internal controls, and audit readiness.

DOJ Data Security Program

In parallel, pursuant to Executive Order 14177 the US Department of Justice implemented its Data Security Program restricting certain data transactions involving "countries of concern." The program distinguishes between prohibited and restricted transactions involving sensitive personal data and US government–related data and imposes security, governance, and recordkeeping obligations on covered entities.

This framework reflects a growing national security overlay in cybersecurity regulation, requiring organizations to reassess their cross-border data flows, vendor relationships, and cloud architectures through both privacy and geopolitical risk lenses.

Incident Reporting Momentum – CIRCIA and Sector-Specific Rules

Federal momentum around incident reporting accelerated in 2025, amplified by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and implementing rulemaking efforts at the Cybersecurity and Infrastructure Security Agency. Adding onto existing sector-specific reporting regimes, proposed rules would require covered entities to report substantial cyberincidents within 72 hours and ransomware payments within 24 hours.

These developments may require organizations to refine intake workflows, escalation thresholds, and cross-functional coordination to ensure timely and accurate reporting across overlapping regulatory obligations.

NIST CSF 2.0 and Incident Response Guidance

The release of NIST's Cybersecurity Framework 2.0 and accompanying incident response guidance further clarified federal expectations around governance-driven cybersecurity programs. With an emphasis on enterprisewide accountability, the updated framework calls for incident response planning that integrates legal, compliance, communications, and executive leadership alongside technical teams.

Organizations are increasingly expected to maintain documented playbooks, define decision-making authority, and coordinate with third-party service providers as part of a mature incident response capability rather than treating response as an ad hoc or purely technical function.

Emerging DOJ Criminal Enforcement Posture

Criminal enforcement activity in 2025 underscored the federal government's willingness to pursue ransomware, insider-enabled cybercrime, and related conspiracies through coordinated investigations. Indictments involving sophisticated ransomware operations highlighted the role of credential misuse, privileged access, and internal control failures.

These cases reinforce the importance of identity and access management, insider risk monitoring, and incident response strategies that anticipate parallel criminal, regulatory, and civil exposure following a significant cyber event.

The Rise of State-Driven Cyber Governance

CPPA Rules on ADMT and Cybersecurity Audits

The California Privacy Protection Agency, the state's privacy regulator, finalized regulations in July 2025 governing automated decision-making technology, cybersecurity audits, and risk assessments, significantly expanding compliance obligations for many businesses. The rules require enhanced transparency, meaningful human involvement, and ongoing assessments where processing presents heightened risk, while also mandating formal cybersecurity audits and reporting for certain high-risk activities.

Notably, the requirements elevate documentation and governance expectations well beyond notice-based compliance.

State AG Activity in Privacy and Cybersecurity Enforcement

State attorneys general continued to assert a leading role in privacy enforcement, with actions targeting digital tracking technologies, health-related data, opt-out requirements, and online consent mechanisms.

In the data security realm, enforcement theories increasingly focused on deceptive practices and inadequate disclosures rather than breach response failures, signaling that cybersecurity and privacy compliance must be aligned with public-facing representations and consumer expectations even in the absence of a data incident.

New State Privacy Laws Take Effect

The effective dates of new comprehensive privacy statutes in states such as Tennessee, Minnesota, and Maryland further accelerated the shift toward a multistate compliance model. In the absence of legislation at the federal level, and after California led the way to create a comprehensive consumer privacy law in 2018, nearly half of the states are now following with laws of their own.

But these laws are not uniform and introduce varying requirements related to security safeguards, risk assessments, and individual rights, adding complexity for organizations operating nationally and reinforcing the need for scalable, jurisdiction-agnostic governance frameworks.

Texas AG Enforcement and Texas 'Mini-TCPA'

Texas enforcement activity highlighted a growing scrutiny of data practices tied to communications, marketing, and emerging consumer protection statutes, including the state's so-called "Mini-TCPA."

These developments signal increased risk for companies operating in telecom, advertising, and digital engagement spaces, wherein data collection and automated outreach practices intersect with privacy and cybersecurity obligations.

Operational Implications

Taken together, state-level developments from 2025 significantly increased the documentation, assessment, and governance burden on organizations, particularly those operating across multiple jurisdictions. Managing overlapping audit, risk assessment, and disclosure obligations has become a core operational challenge, requiring closer coordination between cybersecurity, privacy, legal, and compliance functions.

Entering 2026, organizations should expect regulators to focus less on one-off compliance artifacts and more on whether privacy and cybersecurity programs operate coherently and at scale across jurisdictions.

Sector-Specific Cyber Rules Came Into Focus

Defense Contracting and False Claims Act Exposure

In the defense sector, cybersecurity controls increasingly functioned as contractual gateways rather than ancillary requirements. Under regimes such as the aforementioned CMMC, representations regarding security posture are closely tied to payment eligibility and contract performance, heightening the risk that deficiencies or inaccuracies could give rise to FCA exposure—even absent a successful intrusion.

Consequently, defense contractors and their suppliers must treat cybersecurity compliance as a bid- and performance-stage risk, with misalignment between technical controls and contractual representations creating potential FCA exposure throughout the supply chain.

Healthcare and FDORA Section 524B

Healthcare and life sciences organizations faced expanded cybersecurity obligations under Section 524B of the Federal Food, Drug, and Cosmetic Act, added by the Food and Drug Omnibus Reform Act (FDORA).

These provisions condition approval and continued marketing of certain medical devices on the implementation and maintenance of reasonable cybersecurity controls, elevating cyber risk from a post-market consideration to a core regulatory requirement and creating tension for legacy devices that cannot easily meet modern security expectations.

For medical device manufacturers, these changes elevate cybersecurity to a core element of regulatory compliance, necessitating coordination across engineering, regulatory, quality, and legal teams and increasing exposure where post-market controls fall out of step with evolving security expectations.

Data Centers and Infrastructure Security

Data centers and other critical infrastructure operators continued to sit at the intersection of cybersecurity, privacy, and national security concerns. The fragmented US regulatory landscape—comprising federal rules, state privacy laws, and national security programs—placed renewed emphasis on vendor and subprocessor controls, contractual risk allocation, and embedded technical safeguards as essential components of infrastructure resilience.

This convergence places data center operators at the forefront of regulatory scrutiny, particularly where infrastructure supports sensitive workloads, cross-border data flows, or government and defense customers.

The Litigation Backdrop to Cybercompliance

Pennsylvania Wiretapping Litigation

Litigation under Pennsylvania's Wiretapping and Electronic Surveillance Control Act continued to create uncertainty for companies using website analytics, session replay, or similar technologies. Courts closely examined whether privacy policies and disclosures provided sufficient notice and consent for alleged "interceptions" of communications, with mixed outcomes depending on the specificity and placement of disclosures.

These cases reinforce the notion that compliance risk often turns less on the technology itself and more on how its use is described to consumers and whether consent can be established on a classwide basis.

CIPA Litigation and Proposed Amendments

California Invasion of Privacy Act (CIPA) claims remained a focal point of privacy litigation in 2025, particularly in cases alleging unlawful interception through embedded third-party tools such as chat features, analytics software, and marketing pixels. Courts continued to wrestle with whether routine website functionality constitutes a prohibited "eavesdropping" arrangement under the statute.

Concurrently, proposed legislative amendments aimed at curbing high-volume CIPA class actions signaled potential relief for businesses, but uncertainty around their scope, timing, and retroactive effect kept CIPA exposure a persistent concern.

Class Certification Trends

Several decisions in 2025 continued a trend of heightened judicial scrutiny at the class certification stage in privacy and cybersecurity cases, particularly where claims turned on individualized questions of consent, reliance, or causation. Courts declined to certify classes where plaintiffs could not demonstrate common proof of uniform data practices or user experiences, reinforcing defendants' ability to defeat aggregation through early factual development.

These rulings underscore that technical variability—such as differences in tracking technologies, user settings, or disclosures—can be outcome-determinative at certification.

Damages and Jury Verdict Exposure

2025 also highlighted the continuing risk of substantial damages and settlement pressure where privacy claims survived threshold challenges. In cases that proceeded to trial or advanced beyond dispositive motions, plaintiffs successfully leveraged alleged discrepancies between public privacy statements and actual data practices to support damages theories—even where concrete consumer harm was difficult to quantify.

These outcomes demonstrate that once liability theories take hold juries may be receptive to narratives focused on trust, transparency, and misuse of personal data, increasing downside risk despite unresolved questions around economic injury.

Practical Litigation Impacts

Taken together, the litigation developments of 2025 in the United States have materially influenced how organizations assess cyber and privacy risk. Defense strategies increasingly hinge on early technical fact development, alignment between engineering practices and public disclosures, and careful documentation of consent and data flows. These cases also affected settlement valuation as certification risk and jury exposure diverged sharply depending on jurisdiction and claim theory.

From an enterprise perspective, this litigation environment reinforced that cybersecurity and privacy compliance cannot be siloed from litigation preparedness: incident response planning, vendor management, insurance placement, and disclosure review all play a role in shaping downstream litigation outcomes.

THE UNITED KINGDOM, EUROPE & THE MIDDLE EAST

Europe's Steady March Toward Cyber Resilience

Operational Resilience and Cybergovernance

Across the United Kingdom and European Union, 2025 reflected a steady but consequential shift toward more mature, governance-driven approaches to cybersecurity and operational resilience. Regulatory attention continued to move beyond point-in-time technical controls toward enterprise-level accountability, testing, and documentation, particularly in sectors such as critical infrastructure, financial services, and other regulated industries.

Expectations increasingly centered on whether organizations could demonstrate not only that security measures exist but that they were integrated into risk management frameworks, periodically tested, and subject to senior oversight. This evolution reinforced the importance of cyberresilience as an ongoing operational discipline rather than a compliance checklist.

Digital Markets and Cross-Border Data Transfers

At the same time, cybersecurity obligations in Europe became more deeply intertwined with broader digital regulation, including digital markets rules and cross-border data transfer requirements. Organizations were required to navigate overlapping regimes governing competition, consumer protection, data protection, and security, often using the same underlying technical and organizational measures to satisfy multiple regulatory objectives.

This convergence heightened the importance of coordinated governance across legal, privacy, cybersecurity, and business teams, particularly for companies operating complex cross-border data flows or platform-based business models.

Infrastructure Security and Cloud Supply Chains

Regulators also placed growing emphasis on infrastructure security and cloud supply chain resilience, reflecting concern over systemic risk and concentration in digital services. Rather than focusing solely on an organization's internal controls, regulatory scrutiny increasingly extended to third-party providers, subcontractors, and technology dependencies.

This shift underscored the need for robust vendor risk management, contractual security obligations, and continuous oversight of cloud and infrastructure partners as part of an organization's core cyber risk posture.

The EU AI Act

The adoption and implementation of the EU Artificial Intelligence Act added another layer to this evolving landscape. While not framed as a cybersecurity statute, the EU AI Act's risk-tiered obligations for AI systems reinforced expectations around data governance, transparency, and security by design.

For organizations deploying or developing AI, 2025 marked the beginning of a period in which cybersecurity, privacy, and AI governance could no longer be treated as separate compliance streams.

Looking ahead to 2026, companies should expect regulators to assess cyber resilience through an integrated lens, examining how security controls support not only data protection and infrastructure resilience but also the safe, transparent, and accountable deployment of advanced digital and AI-enabled systems.

The Middle East's Cyber Modernization Push

Infrastructure and Energy Sector Focus

Across the Middle East, cybersecurity and operational resilience continued to be treated as core elements of infrastructure and energy policy in 2025, reflecting the strategic and economic importance of these sectors. Regulatory frameworks increasingly emphasized system availability, incident response preparedness, and the protection of industrial and operational technology environments alongside traditional IT systems.

For organizations operating in energy, transportation, and other critical infrastructure sectors, cybersecurity expectations were closely tied to business continuity and national resilience objectives, reinforcing the need for integrated cyber and operational risk management.

Contracting and Data-Handling Obligations

Cybersecurity obligations in the region increasingly manifested through contractual and data-handling requirements, particularly in cloud, outsourcing, and managed services arrangements. Regulators and counterparties alike placed greater emphasis on security representations, audit rights, incident notification provisions, and flow-down obligations to subcontractors and service providers.

These developments have placed added pressure on multinational compliance programs to standardize contractual protections and governance frameworks across regional operations while accommodating jurisdiction-specific regulatory expectations.

Geopolitical and National Security Sensitivity

Heightened geopolitical risk continued to shape cybersecurity and data governance expectations throughout the Middle East, particularly for organizations managing cross-border data flows or centralized digital platforms. Regulatory scrutiny increasingly reflected concerns around data sovereignty, access controls, and the resilience of systems supporting sensitive governmental or critical commercial functions.

As a result, cybersecurity compliance in the region often intersects with national security considerations, requiring companies to evaluate both technical safeguards and organizational and architectural decisions affecting data access and control.

UAE and Saudi Privacy Law Developments

In 2025, implementation of the UAE Personal Data Protection Law and amendments to Saudi Arabia's Personal Data Protection Law underscored a broader regional trend toward modernization and alignment with global data protection principles while retaining distinct local features. These regimes expanded obligations around security safeguards, cross-border transfers, and accountability, with enforcement frameworks continuing to take shape.

For companies operating in or throughout the region, these developments increase the importance of localization strategies, compliance readiness, and ongoing monitoring, particularly as regulators move from implementation to enforcement in 2026.

ASIA

China's Expanding Cyber Rulebook

Incident Reporting Requirements

China's National Cybersecurity Incident Reporting Management Measures, which took effect in November 2025, have significantly formalized incident response expectations by introducing severity-based reporting thresholds and detailed procedural requirements. Covered entities are expected to maintain documented response plans, conduct regular training, and coordinate closely with service providers and vendors when incidents occur.

The measures emphasize organizational preparedness and escalation discipline as much as technical remediation, signaling that regulators will assess how incidents are identified, classified, and reported—and not just how they are fixed—when evaluating compliance.

Outbound Transfer Certification

Certification-based mechanisms under China's Measures for the Certification of Personal Information Outbound Transfer expanded available compliance pathways while maintaining strict regulatory oversight.

These certification-based mechanisms apply only to noncritical information infrastructure operators meeting specific volume thresholds (100,000–1 million nonsensitive personal information subjects, or less than 10,000 sensitive personal information subjects per calendar year) and exclude "important data" from certification-based mechanisms. The mechanisms require organizations to implement robust governance structures, execute compliant contractual arrangements, and conduct ongoing assessments of data protection practices.

For multinational companies, certification offers greater flexibility than case-by-case approvals but it also demands sustained internal controls and documentation, particularly where data flows involve affiliates, shared service centers, or external processors.

Data Localization Impacts

Taken together, China's incident reporting and data transfer frameworks continued to complicate data localization and cross-border operational models in 2025. Organizations relying on centralized analytics, regional cloud platforms, or global security monitoring functions increasingly faced pressure to segment systems, localize processing, or implement enhanced access controls.

These constraints reinforce the need for early architectural planning and close coordination between cybersecurity, IT, and legal teams when designing or modifying China-related data environments.

Cybersecurity Law Amendments and 'Important Data'

Amendments to China's Cybersecurity Law and the expansion of "important data" catalogs further increased the scope of regulated information subject to heightened protection. The evolving definitions of covered data categories have forced organizations to revisit data inventories, classification methodologies, and transfer strategies on an ongoing basis.

As regulators continue to clarify expectations through implementing standards and enforcement activity, companies in 2026 face sustained pressure to demonstrate defensible, well-documented data governance frameworks that can adapt to shifting regulatory interpretations.

Asia Pacific Moves Toward Cyber Alignment

Across the Asia-Pacific region, 2025 saw continued development of cybersecurity and data governance frameworks aimed at strengthening resilience in cloud operations, breach response, and cross-border processing. While regulatory approaches varied by jurisdiction, a common theme emerged around formalizing organizational accountability for cyber risk and integrating security expectations into broader digital governance regimes.

For companies operating regionally, this trend increases the importance of harmonizing internal controls to meet diverse but increasingly structured local requirements.

Hong Kong Infrastructure Cybersecurity Ordinance

Hong Kong's Infrastructure Cybersecurity Ordinance, which took effect January 1, marks a shift toward a more centralized and formalized regulatory model for protecting critical infrastructure. The ordinance places clear obligations on designated operators to implement security controls, conduct risk assessments, and report incidents, with a focus on organizational responsibility and governance.

Its adoption signals that infrastructure resilience is now a more prominent regulatory priority in the region, particularly for sectors supporting essential services and digital connectivity.

Convergence Around Global Norms

Regional frameworks across Asia Pacific continued to converge around global cybersecurity and incident reporting norms, even as implementation details remained jurisdiction-specific. Many regulators emphasized principles such as risk-based controls, timely incident reporting, and third-party risk management, aligning local requirements with international standards.

This convergence offers some opportunity for operational consistency, but it also requires careful mapping of global frameworks to local compliance obligations.

Cyber/AI Integration in Innovation Policy

Governments across the region are increasingly embedding cybersecurity and artificial intelligence considerations into national innovation and economic development strategies. These initiatives reflect growing recognition that digital trust and system security are prerequisites for sustainable innovation.

For organizations deploying advanced technologies, this integration signals that cybersecurity governance will play a strategic role not only in regulatory compliance but also market access and participation in government-supported innovation ecosystems as 2026 approaches.

LOOKING AHEAD

In 2025, the cybersecurity landscape continued to diversify across federal rules, state statutes, enforcement actions, and private litigation outcomes in the United States, while the United Kingdom, European Union, and Middle East advanced harmonized approaches to operational resilience, AI governance, and infrastructure security. In China and across Asia Pacific, incident reporting, data transfer controls, and infrastructure cybersecurity obligations deepened regulatory complexity for global organizations.

Looking ahead to 2026, implementation and enforcement are expected to intensify. Cross-border AI accountability challenges, particularly around training data, model provenance, copyright, and automated decision-making, are likely to intersect increasingly with cybersecurity and privacy regimes. Ransomware

prosecution and criminal enforcement tied to nation-state and insider activity are also expected to remain prominent.

Organizations that invest in integrated, well-documented cybersecurity programs grounded in governance, contractual controls, and incident readiness will be best positioned to manage this evolving risk environment.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Boston		
Heather Egan	+1.617.341.7733	heather.egan@morganlewis.com
Dubai		
Ksenia Andreeva	+971.4.312.1865	ksenia.andreeva@morganlewis.com
Houston		
Catherine North Hounfodji	+1.713.890.5120	catherine.hounfodji@morganlewis.com
Los Angeles		
Megan A. Suehiro	+1.213.612.7324	megan.suehiro@morganlewis.com
London/Brussels		
Vishnu Shankar	+44.20.3201.5558	vishnu.shankar@morganlewis.com
Philadelphia		
Ezra D. Church	+1.215.963.5710	ezra.church@morganlewis.com
Kristin M. Hadgis	+1.215.963.5563	kristin.hadgis@morganlewis.com
Gregory T. Parks	+1.215.963.5170	gregory.parks@morganlewis.com
Shanghai		
Todd Liao	+86.21.8022.8799	todd.liao@morganlewis.com
Washington, DC		
Hannah Levin	+1.202.739.5896	hannah.levin@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

Connect with us

www.morganlewis.com