

HOT TOPICS IN CYBERSECURITY: DATA BREACHES, INCIDENT RESPONSE, AND THE CURRENT LEGAL LANDSCAPE

September 25, 2026





Amy de La Lama
Chair, Global Data Privacy
& Security



Jeffrey Schultz
Chair, Data Innovation,
Security and Privacy Practice



Armstrong
Teasdale



Jeff Tucker
Senior Corporate Counsel
Global Legal Department



Enterprise Mobility™

Welcome and Introductions

Agenda

01 How Do Data Breaches Happen?

02 Average Cost of a Data Breach

03 Lifecycle of a Data Breach

04 The Emerging Role of AI

05 Ransomware: Current Trends

06 Ransom Payment Considerations

07 Law Enforcement Reporting – Timing Considerations

08 Challenges Posed by the Patchwork of US Laws (State and Federal)

09 Current State of Data Breach Litigation

10 What questions should we be asking? / Questions

How Do Data Breaches Happen?



Average Cost of a Data Breach



2026 COST
BENCHMARK

COMPARATIVE BREACH COST

GLOBAL



\$4.99 million

AI ENABLED



\$6.0 million

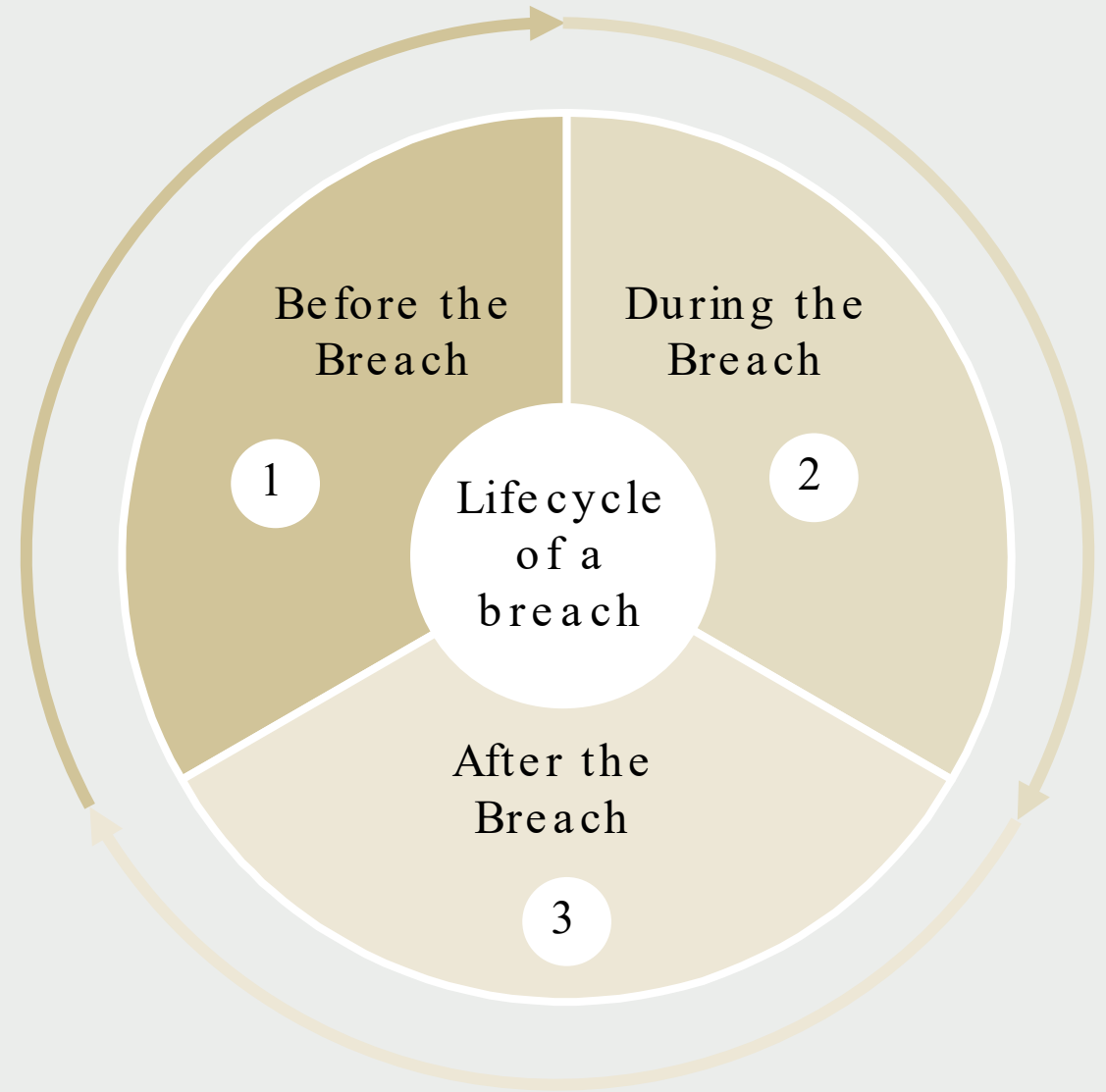
US



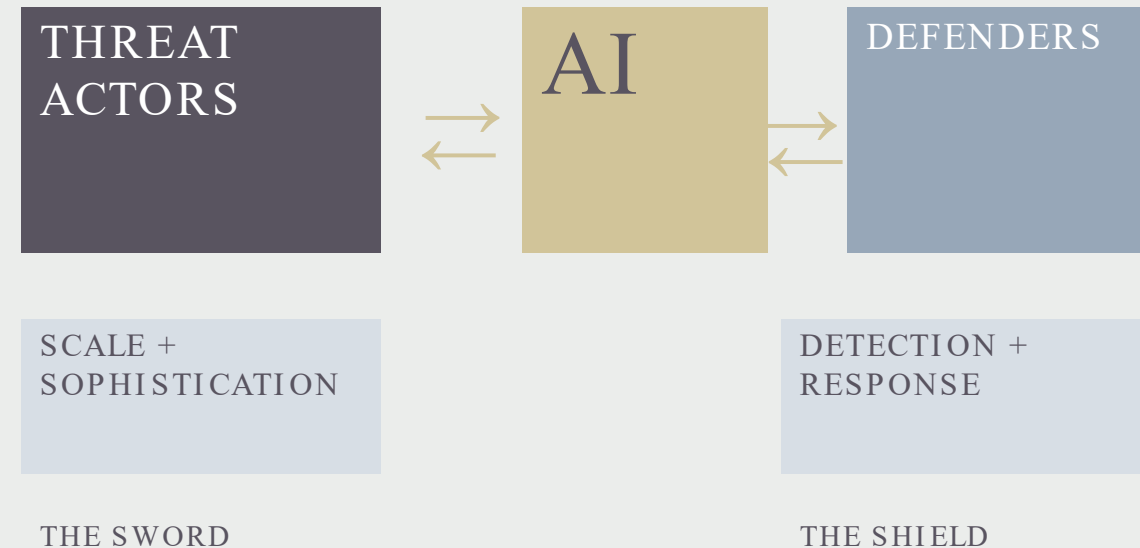
\$11.5 million

Source: [IBM Cost of a Data Breach Report 2026: The AI Oversight Gap](#)

LIFECYCLE OF A DATA BREACH



THE EMERGING ROLE OF AI



AI accelerates both attack capability and defensive resilience.

The Sword: How Threat Actors Use AI

A person wearing a dark hoodie is sitting at a desk, using a laptop. The laptop screen displays the letters 'AI' in a bright blue, glowing font. The person's face is obscured by the hood. The background is dark and filled with glowing digital lines and circuitry, suggesting a high-tech or cyber environment. The overall tone is mysterious and technological.

AI used to scale attacks (frequency and sophistication)

Generative AI and social engineering

- Personalized phishing
- Deepfakes
- Malware
- DDoS attacks

The Shield:

How organizations use AI for defense

- The global AI cybersecurity market is projected to top \$134B by 2030.
- Organizations are using AI-powered tools for **threat detection, automated response, and vulnerability management**



Ransomware: Current Trends

THREAT ECONOMICS

Attack Frequency: Activity remains at or near record levels

Victim Payment Rates: Sharply declining, driven by:

- Improved backup and recovery capabilities
- Payment does not guarantee data deletion or non-publication
- More aggressive law enforcement action (takedowns, seizures, sanctions designations)
- Regulatory and legal scrutiny of payments (notably OFAC sanctions exposure)
- Cyber insurers imposing stricter security-control and coverage requirements

LEGAL + OPERATIONAL OVERLAY

Data-Theft (Double) Extortion Now Dominant: Threat actors increasingly exfiltrate data before encrypting systems and use the threat of publication as independent leverage

Primary Access Methods: Credential theft, social engineering (e.g., phishing), and identity-based attacks are the leading vectors for initial access

Legal and Regulatory Overlay:

- OFAC/ sanctions risk: Facilitating a ransom payment to a sanctioned actor can violate U.S. sanctions under IEEPA; strict-liability exposure; civil penalties up to the greater of \$1M or 2x the pecuniary gain or loss
- Federal reporting (CIRCA): Once CISA's final rule takes effect, covered critical-infrastructure entities must report covered cyber incidents to CISA within 72 hours and ransom payments within 24 hours
- Payment is not a cure: Refusal or payment can each still result in permanent data loss and downstream litigation

Ransom Payment Considerations

1 Maintain flexibility –
decision will be
fact dependent

2 Avoid making
unchangeable
policy decisions in
advance but do
include in preparation
activities

3 Engage third party
expert to minimize
further risk

4 Additional considerations

- Regulatory compliance (OFAC, etc.)
- Ability to conduct business operations
- Reputational issues

Law Enforcement Reporting – Timing Considerations

Demonstrates effort to take all available steps to remediate breach

Law enforcement may not be able to prioritize depending on the circumstances

Can slow reporting timelines if requested by law enforcement

Challenges Posed by the Patchwork of US Laws (State and Federal)



Current State of Data Breach Litigation

01



CLASS

Data Breach Class Actions

- Standing: TransUnion concrete-injury requirement; circuit split on risk-of-future-harm
- Causation nexus and individualized injury
- Rule 23(c)(4) issue classes (duty/breach common; causation individualized)

02



COMMON LAW

Common-Law Claims

- Negligence / negligence per se
- Breach of contract / implied
- Unjust enrichment
- Intrusion upon seclusion

03



STATUTORY

Statutory Private Actions

- VPPA pixel-tracking claims
- ECPA/Wiretap Act interception
- CIPA pen register/wiretap
- State wiretap analogs

04



EMERGING

New Laws / Emerging Claims

- BIPA (biometrics) + 2024 amendment
- AI data-use claims
- Healthcare/financial pixel tracking
- Dark patterns enforcement

— Common-law, statutory, and emerging theories converge in modern breach litigation —

What questions should we be asking?

Do we have robust data security policies and are we complying with them?	Do our public disclosures, policies, and statements match actual practices?	Is leadership paying attention to cybersecurity?	Does our incident response program factor in global compliance obligations?
Do employees know how to avoid common threats (appropriate training)?	Are our vendors secure and do agreements with those vendor address security requirements?	Is our cyber-insurance coverage adequate and do we know how to estimate our risk exposure?	Have we factored in risks specific to the M&A context?

QUESTIONS

