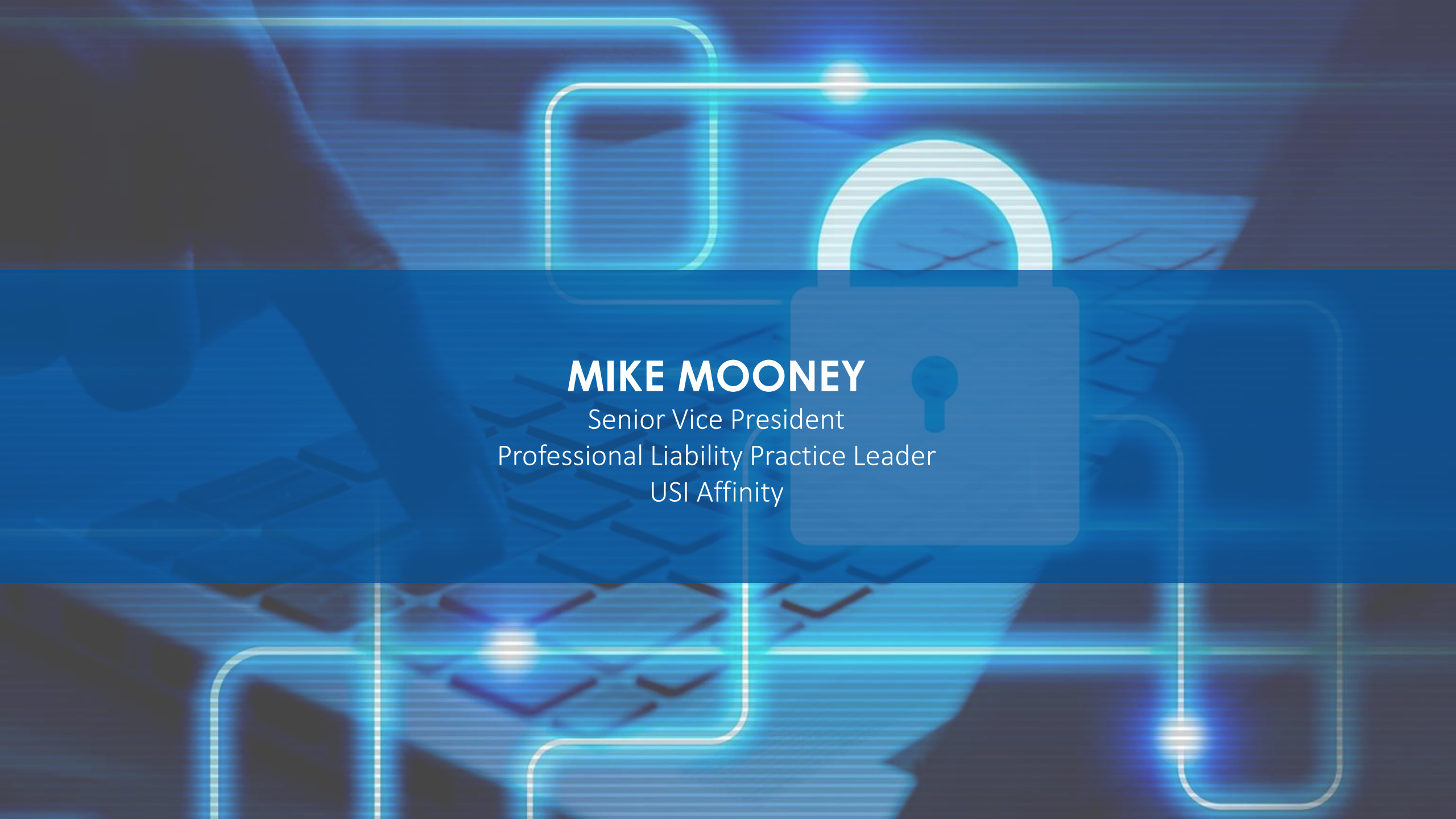
USI SOLUTIONS FOR COMMERCIAL RISK MANAGEMENT

April 2026

NAVIGATING THE CYBER WORLD: RISK MITIGATION FOR LAW FIRMS

THE USI ONE ADVANTAGE®

www.usi.com



MIKE MOONEY

Senior Vice President
Professional Liability Practice Leader
USI Affinity

Agenda

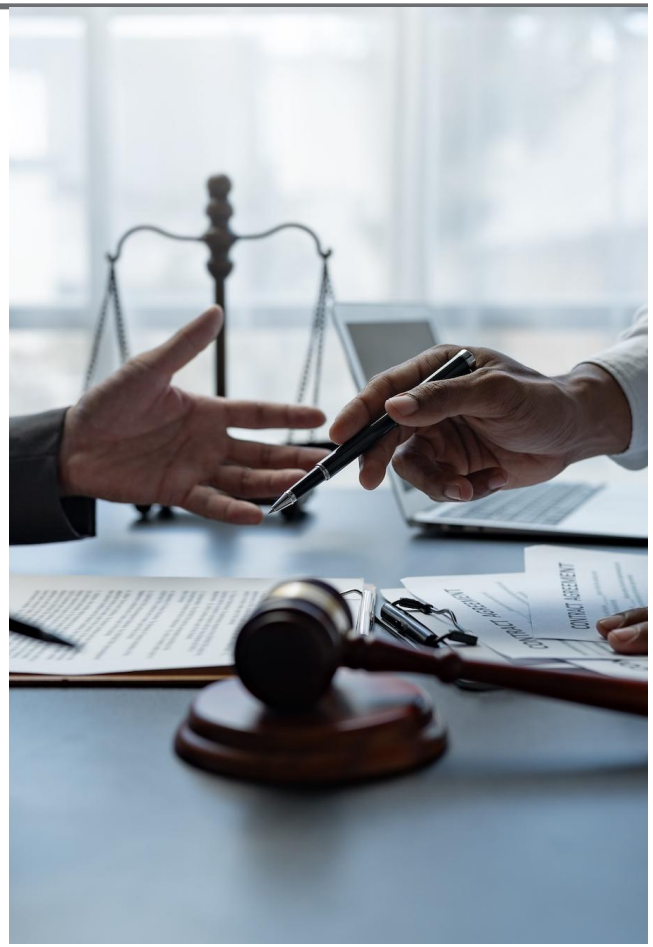
- Why Law Firms?
- Cyber Claims & Losses
- Competence and Diligence
- Cyber Insurance
- Risk Management

Target Rich Environment

- Law Firms provide access to valuable and confidential client data
- Intellectual Property / High Value Data
- High Value Transactions
- Heavy reliance on email
- Poor Cybersecurity Practices
- Breaches carry major business consequence
- Business Intelligence / M&A
- Protected Health Information (PHI)
- Bank Account and Credit Card Information (PCI)
- Personally Identifiable Information (PII)

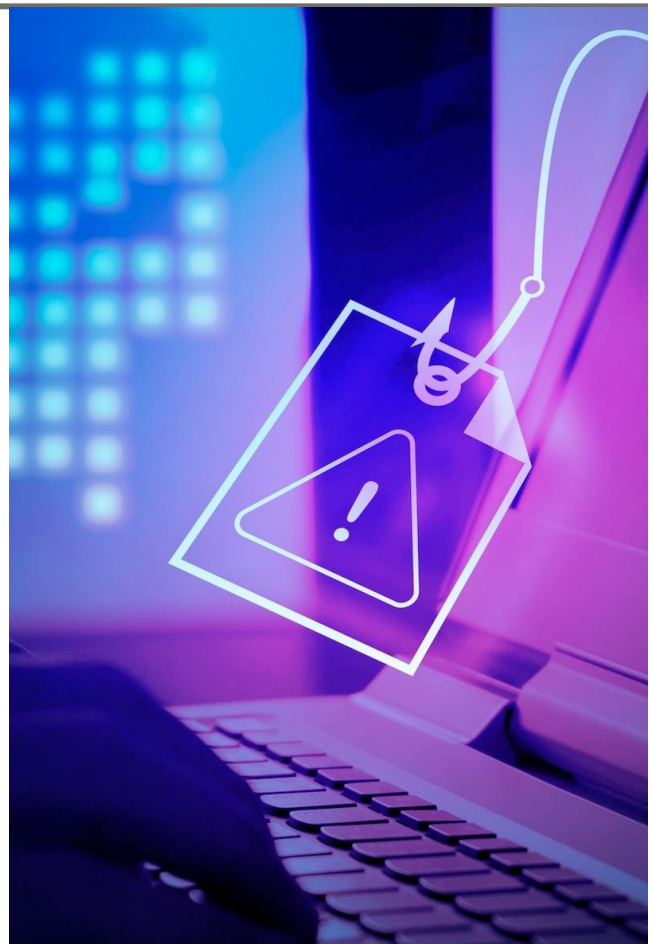
Why Law Firms fail to take adequate security measures

- Lack of Cybersecurity Awareness
- False sense of Security
- Overreliance on 3rd Party Vendors & IT Providers
- Insurance is Too Expensive
- Human Vulnerabilities / Training Gaps
- Unclear Regulatory Requirements



Most Common Cybersecurity Threats for Law Firms

- Phishing Scams & Social Engineering
- Ransomware Attacks
- Business Email Compromise
- Data Breach & Unauthorized Access
- 3rd Party & Vendor Vulnerabilities
- Remote Work & Unsecured Devices



Top 5 by Number of Claims

- Ransomware
- Business Email Compromise
- Funds Transfer Fraud
- Hacking / Unauthorized Access
- Staff Mistakes

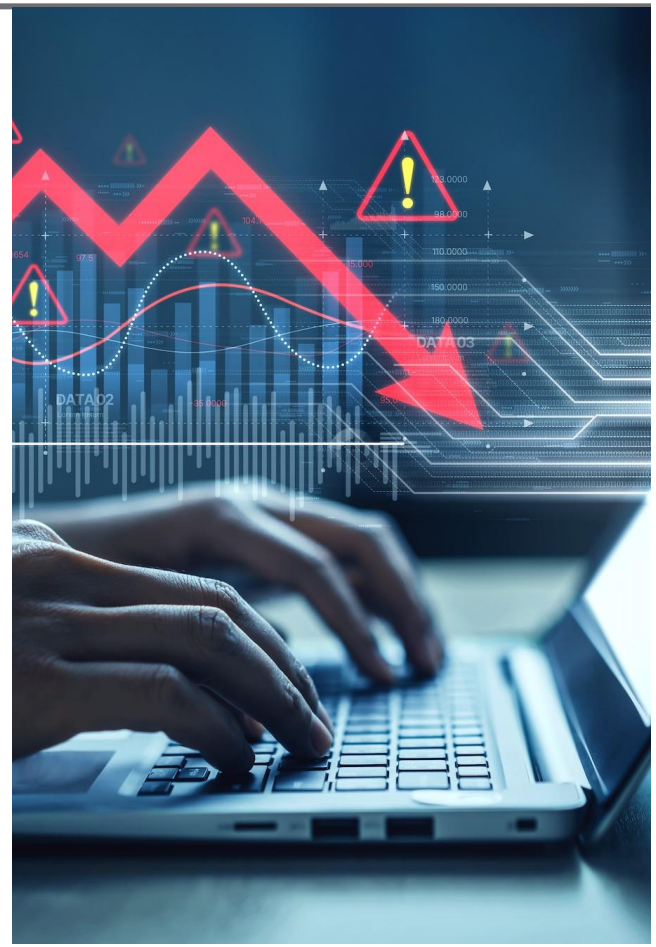
High Cost of a Data Breach

- 20% of all law firms experienced a cyberattack in the past year.
- 56% of all firms that suffered a break lost sensitive client information.
- Average cost of a data break for a law firm is $5.08 million. (10% increase yoy)
- Average cost of a breach for a small firm is $36,000.
- 65% firms are unfamiliar with their legal obligations following a breach.
- 34% of law firms report having an incident plan in place, down from 42% the previous year.
- The legal industry faces an average of 1,055 attacks per week. (13% increase yoy)
- 10% of law firms have no one monitoring their cybersecurity, either in-house or third party.

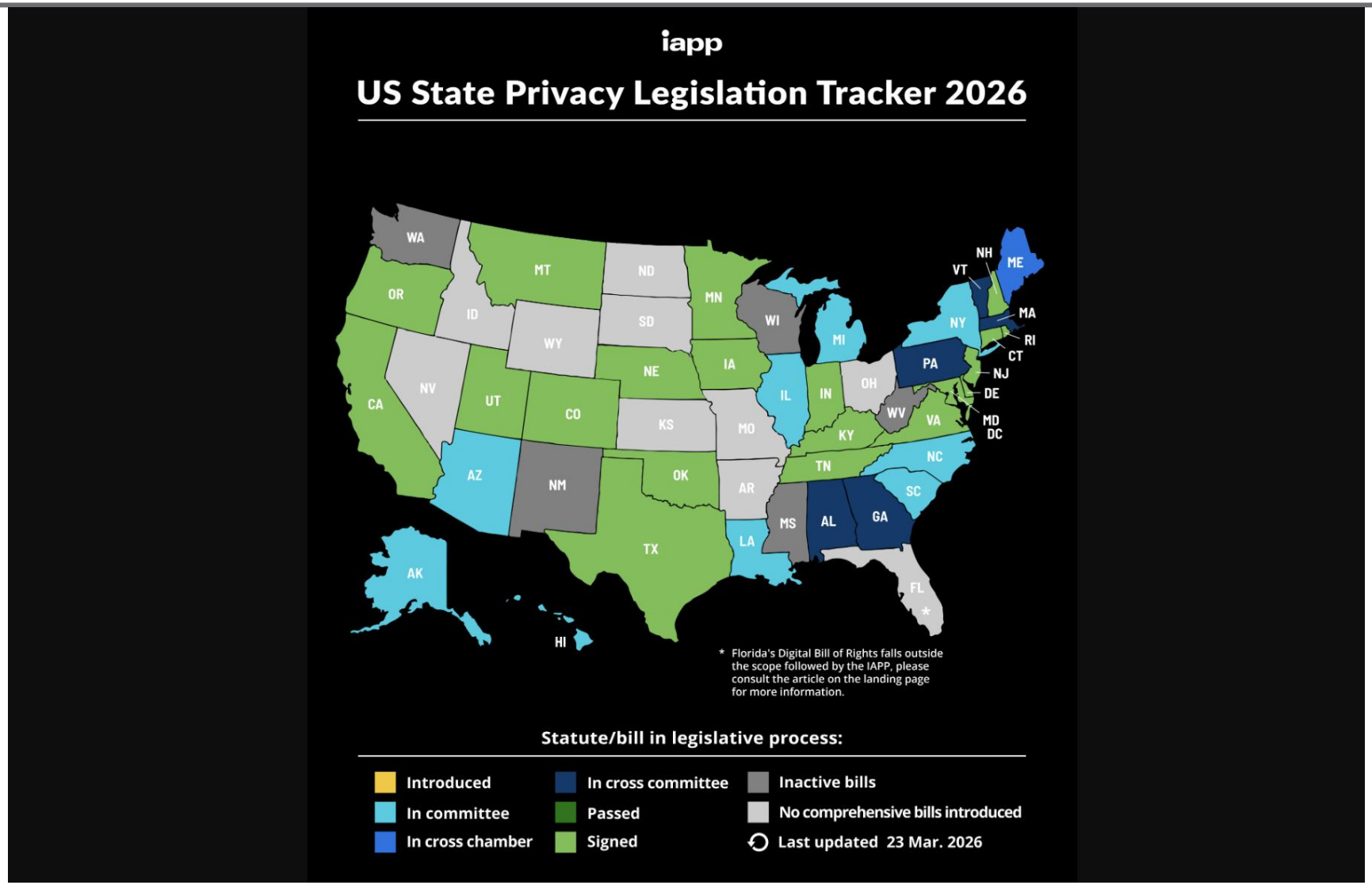
2026 Programs.com

Cyber Exposures – Cyber Loss

- Financial Losses
- Legal & Regularity Exposure
- Reputational Damage
- Litigation Costs
- Loss of Clients
- Loss or damage to reputation
- Operational Disruption



Competence and Diligence



Source: iapp

Competence and Diligence

- Model Rule 1.1 – Competence (including Technology)
- Model Rule 1.6 – Confidentiality of Information
- Model Rule 1.4 – Keeping clients "reasonably informed"
- Model Rule 1.15 – Safeguarding Client Property (applies to digital client files & Data)
- Opinion 477R – Securing communication of protected client information
- ABA Opinion 483 – Obligations to Clients after a Data Breach

Insurance Coverage Parts

Comprehensive Cyber Coverage has (3) Distinct Coverage Parts:

- 1st Party restoration,
- 3rd Party protection, and
- Services: Cyber event services to assist companies if there is an event

Coverage Misconceptions

- Our General Liability Policy covers Cyber…"
  - Most CGL policies explicitly exclude cyber relates losses.
- "Property Insurance covers Cyber…."
  - Property policies typically require direct physical loss or damage.
- "Crime policies cover social engineering and Cyber…"
  - Normally covers employee theft.
- "Business interruption coverage includes Cyber…"
  - Traditional BI coverage is triggered by physical damage to insured property.
- "My LPL covers Cyber…"
  - Some coverage. Will never cover first party losses.
- "My D&O policy covers Cyber…"
  - Won't cover the Breach itself. May cover allegations of mismanagement after a breach.
- "We're too small to need separate Cyber coverage…."

Coverages

- Choice of counsel
- Pay on behalf of language
- Funds Transfer Fraud
- Ransomware (submits & deductibles)
- Business Interruption (waiting times)
- Data Recovery & Restoration
- Reputational Harm / Reputational Loss
- Risk Management Offerings

Risk Management

- Use common sense
- Strong Data Encryption Practices
- Adopt Multi-Factor Authentication (MFA)
- Strong Password Management
- Develop Incident Breach Response Plan
- Employee Training & Education
- Limit user access to only data and systems necessary for their role
- Regularly Software Updates & Patching
- Complete a Risk Analysis
- Buy Cyber Insurance

Thank you for attending today's seminar.

We hope that you found it informative.

Mike Mooney

Senior Vice President

Professional Liability Practice Leader

USI Affinity

Mike.Mooney@usi.com

610.537.1441