



# Cyber Insurance: Multifaceted Coverages for Multifaceted Risks

*August 14, 2024*

---

The information and opinions expressed by our panelists today are their own, and do not necessarily represent the views of their employers or of PLUS.

The contents of these materials may not be relied upon as legal advice.

Please submit your questions through the “Q&A” tool on user dashboard.

# Today's Session

---

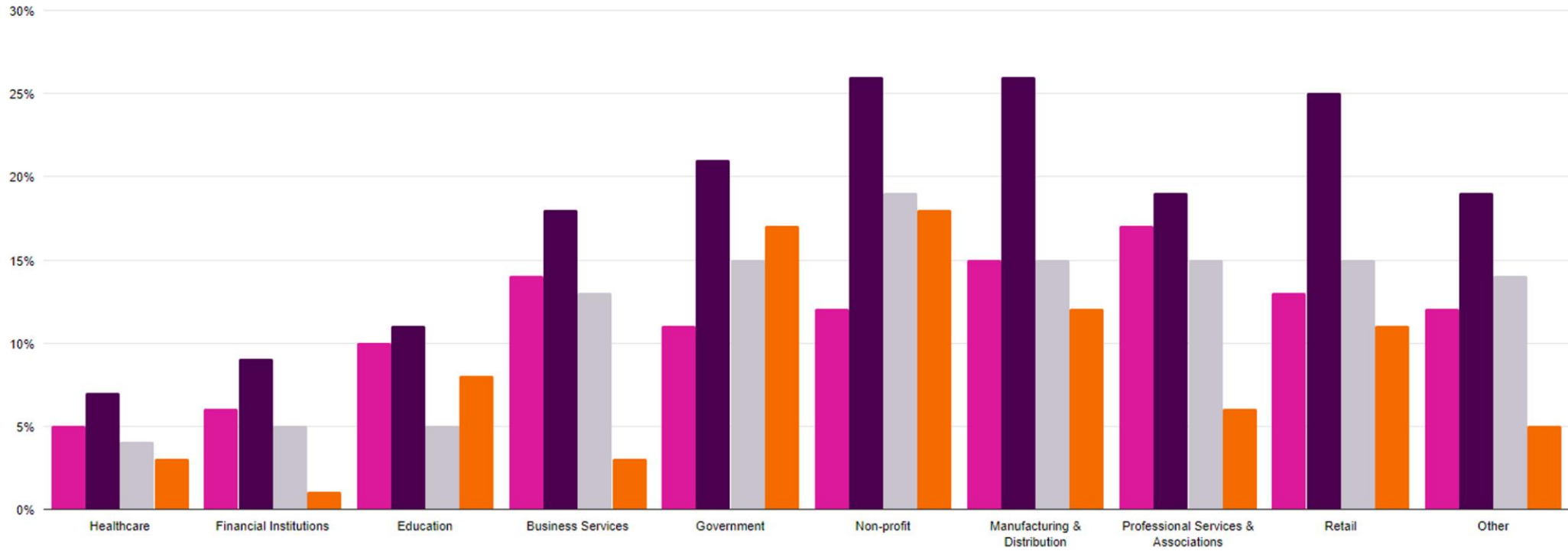
- Types of Risks
- Sources of Legal Exposures
- Effects on Policyholders
- Risk Transfer through Insurance

# Current Cyber Threats – Fraudulent Instruction

## Fraudulent instruction as a cause of loss

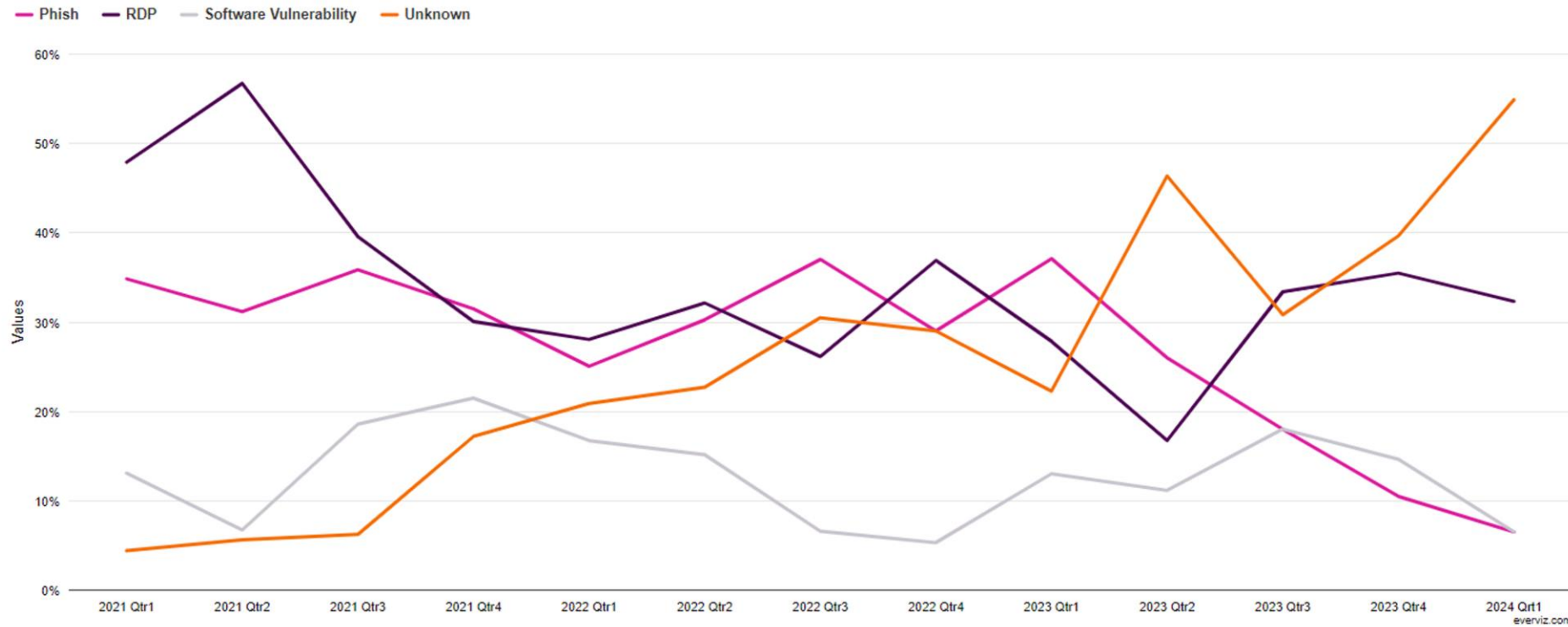
Percentages by industry

■ 2021 
 ■ 2022 
 ■ 2023 
 ■ 2024 Q1



# Current Cyber Threats - Ransomware

Ransomware Vectors

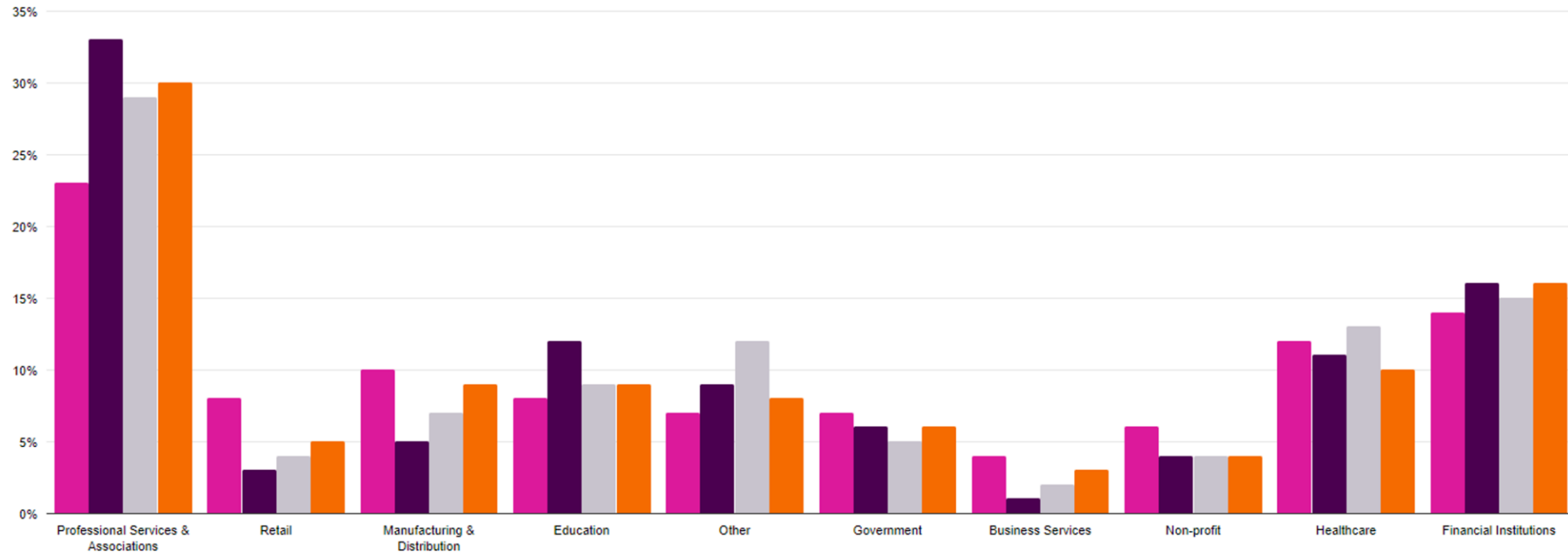


# Current Cyber Threats – Business Email Compromise

## Business email compromise

Percentages by industry

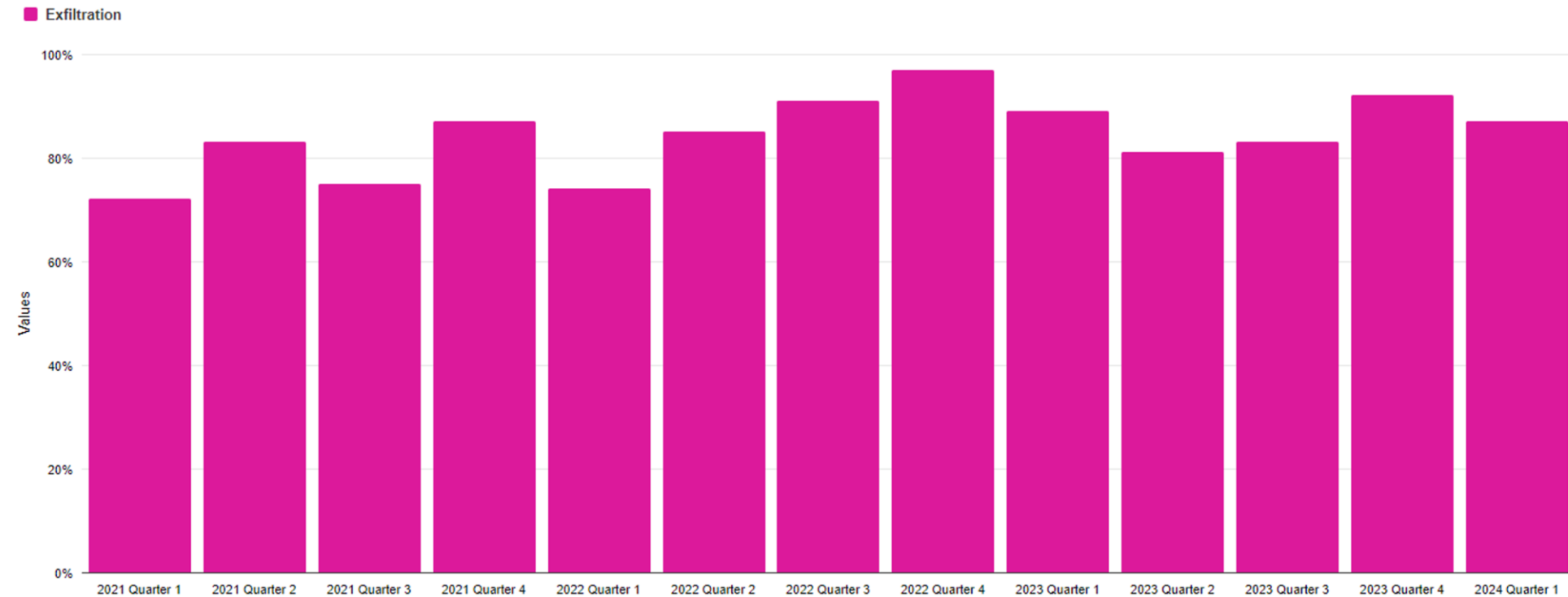
■ 2021 ■ 2022 ■ 2023 ■ 2024 Q1



# Data Exfiltration – Cyber Extortion

## Cyber Extortion Incidents with Data Exfiltration

Percentages by quarter.



# Modern Regulatory Environment

---

- Different sources for laws or standards
  - Federal, state and international law (statute and regulation)
  - Adversarial or enforcement proceedings
  - Some laws are specific to type of industry
  - Some laws are specific to type of information
  - Some industries have developed standards
- Different enforcement mechanisms or pressures
  - Regulatory proceedings
  - Litigation
  - Contractual
  - Stakeholder
  - Marketplace
  - The entity

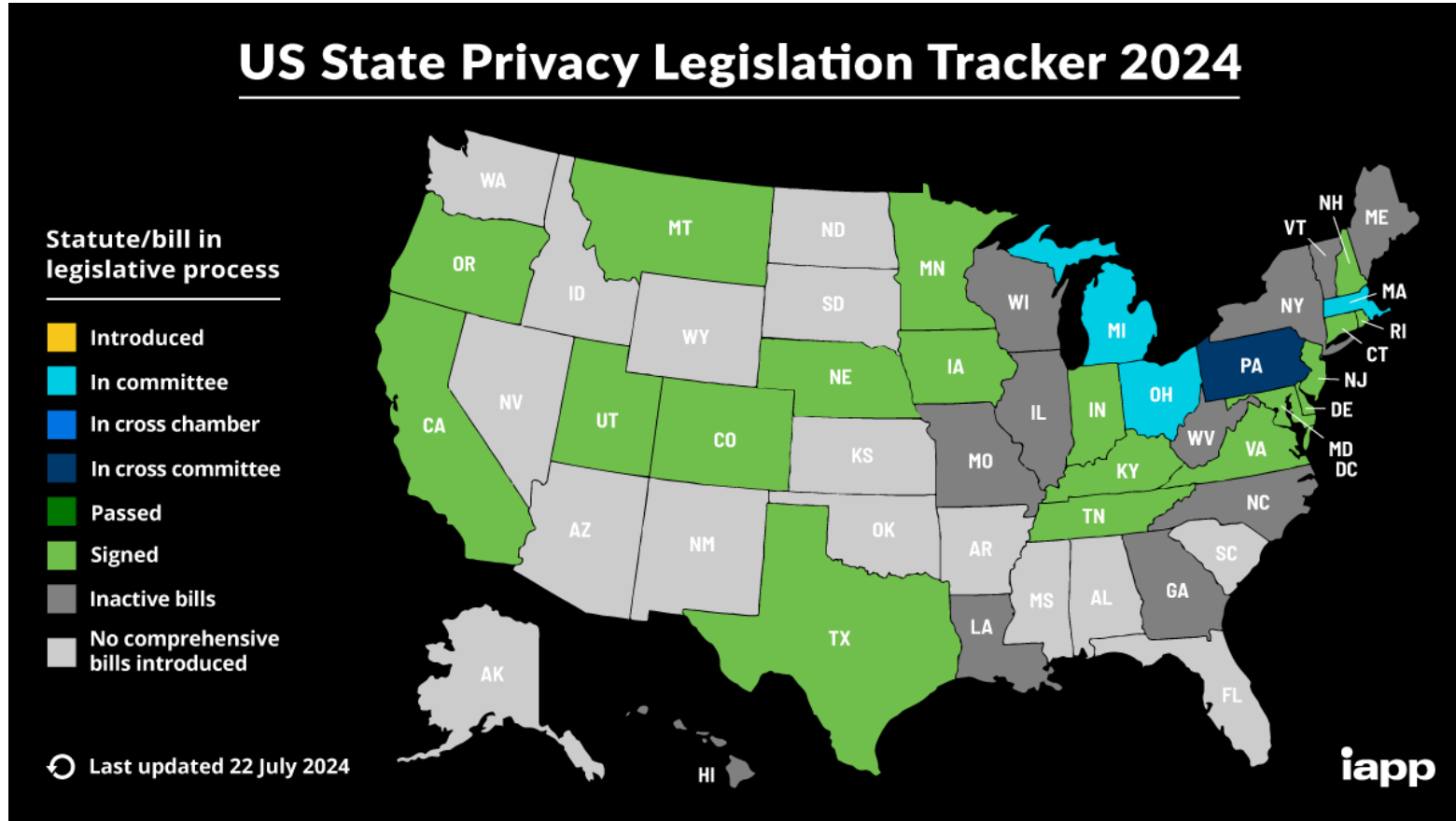


# Government Law

---

- Privacy, cybersecurity - - or both
- Federal, state, non-U.S. - - or “all of the above”
  
- States
  - Each state has a data breach notification law
  - Some states require reasonable security procedures (e.g., MA)
  - Some states have industry-wide requirements (e.g., NY DFS)
  - Some states have laws governing record disposal or destruction
  - Some states protect biometric information privacy (e.g., IL BIPA)
  - Some states have enacted broad privacy protection laws (19 total with 7 being signed in 2023 and another 7 already in 2024)

# Status of state privacy laws



[https://iapp.org/media/images/resource\\_center/State\\_Comp\\_Privacy\\_Law\\_Map\\_2024.png](https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map_2024.png)



# Government Law

---

## ➤ Federal

### ➤ Federal steps and efforts

- Draft American Privacy Rights Act (2024)

- Cyber Incident Reporting for Critical Infrastructure Act of 2022

- Joint Ransomware Task Force

- Many agencies have or assert authority over privacy and cybersecurity issues

- Jurisdictions may be as to certain industries or data

- Authorities may overlap / be concurrent

- Alphabet soup of agencies and laws

- DOJ, DOD, FTC, OCR, SEC, HHS, DOJ, FDA ....

- HIPAA, HITECH, GLBA, COPPA, FRCA, FACTA, FISMA, FERPA, TCPA, ....

# Government Law

---

- Non- U.S.
  - EU-GDPR (eff. 5/25/18). Key GDPR provisions:
    - Higher fines, based on prior year revenues
    - Individual right to seek compensation
    - Broader personal data definition: “information relating to an identified or identifiable natural person” through “all means reasonably likely to be used”.
    - Data breach notification (within 72 hours)
    - Greater data subject rights including right to access, rectify or erase data.
  - Enforcement track record
  - Others (China, Australia, Canada and more)

# Adversarial or Enforcement Proceedings

---

- Litigation arising out of an incident or practice
  - Such as data breach, M&A, IP, business email compromise, wire transfer fraud, ransomware, or indemnification
  - Involving, for example, consumers, shareholders, Ds&Os, management, vendors, commercial partners, transaction parties, and rights-holders
  - individual, mass or class action / arbitration
  - issues of standing, certification, liability and damages
- Litigation arising out of regulatory violations
  - for example, Illinois' Biometric Information Privacy Act, CCPA
- Note: interplay with other sources (e.g., broader consumer protection laws; safe harbor laws; industry or other standards)

# Examples of Recent Regulatory and Civil Activity

## Regulatory

- Texas AG: \$1.4B settlement with Meta under TX's Capture or Use of Biometric Identifier Act ("CUBI") for Facebook's use of facial recognition software (July 2024)
- California AG: secured \$375,000 and injunctive relief against DoorDash under CCPA and other laws for sale of personal information and lack of compliant policies (February 2024)
- SEC: \$487,616 fine against title insurance company for insufficient cyber disclosure controls (June 2021); \$3M fine against software company for making allegedly misleading disclosures about a cyber attack
- FTC/DOJ: \$5.1MM fine (HIPAA) against health insurer following data breach affecting 9.3MM people (January 2021); settlement with Blackbaud requiring data deletion and a comprehensive information security program (February 2024)

## Civil

- \$380.5MM Equifax class action data breach settlement (upheld on appeal June 2021)
- \$650MM settlement against Facebook for alleged violations of the Illinois Biometric Information Privacy Act ("BIPA") (February 2021)
- \$85MM settlement against Zoom for "Zoombombing" (July 2021)
- \$190MM Capital One settlement arising out of 2019 data breach (December 2021)
- \$228MM for BIPA violations against BNSF Railroad (Oct 2022)[new trial awarded July 2023; settled February 2024 for \$75MM]
- \$17B potential damages against White Castle for BIPA violations (February 2023, rehearing denied July 2023; settled May 2024 for \$9.4MM)

# A Policyholder's Possible Losses and Challenges

---

➤ First-Party

➤ Third-Party

➤ Resources for Experienced Assistance



# Cyber Insurance Market Conditions

---

- **Capacity**
  - Could reach US\$43 billion in premiums by 2030 (Howden). More types of vehicles being introduced or considered.
- **Coverages**
  - Market fluctuations concerning size of limits, use of sublimits, incentives, coinsurance, size of retentions, insuring agreements offered, and exclusions included
- **Underwriting**
  - Robust application process, some supplemental applications required, some refusals to quote – enhanced security controls being required
- **Pricing**
  - Cyber premium price increases of 0.7% in Q1 2024, as compared to 8.4% in Q1 2023. (CIAB index)
- **Claims**
  - Cost of Cyber claims including long-tail exposure

# The 3 Pillars of Cyber Insurance

---

## **BREACH RESPONSE COVERAGE**

Forensics

Legal

Notification

Public Relations

Crisis Management

## **FIRST PARTY COVERAGE**

Cyber Extortion

Business Interruption

Dependent Business  
Interruption

Data Recovery

E-Crime

## **THIRD PARTY COVERAGE**

Data & Network  
Liability

Regulatory

PCI

Media Liability

# Insuring Agreements

---

## Breach Response Coverage:

**Privacy Breach Responses Costs:** Coverage includes the fees and costs for legal, forensics, notification, call center, credit monitoring, and public relations / crisis management in response to an actual or reasonably suspected data breach or security breach.

# Insuring Agreements

---

## First Party Insuring Agreements:

- **Cyber Extortion:** Coverage includes reimbursement for an extortion payment and reasonable and necessary expenses incurred with prior consent to prevent or respond to an extortion threat.
- **Cyber Business Interruption:** Coverage includes reimbursement for income loss, extra expense, and forensic expenses from an actual interruption of business operations due to a security breach or system failure.
- **Dependent Business Interruption:** Coverage includes reimbursement for income loss, extra expense, and forensic expenses from an actual interruption of business operations caused by a vendor's security breach or security breach.
- **Data Recovery:** Coverage includes reimbursement for reasonable and necessary costs to regain access, replace, or restore data that cannot be accessed due to a cyber attack.
- **E-Crime and others:** Examples include coverage for social engineering fraud, fraudulent funds transfer, telephone fraud, invoice manipulation, and reputational loss

# Insuring Agreements

---

## Third Party Insuring Agreements:

- **Data & Network Liability:** Coverage for defense and indemnity resulting from a claim for a data breach, security breach, failure to disclose a data or security breach, or failure to comply with certain parts of a privacy policy.
- **Regulatory Defense and Penalties:** Coverage for defense costs and fines/penalties for violations of privacy regulations including but not limited to HIPAA, the Red Flags Rule and the Hi-Tech Act.
- **Media Liability:** Coverage for both certain claims alleging copyright/trademark infringement or libel/slander for media content displayed to the public.
- **Payment Card Liabilities and Costs:** Coverage includes reimbursement for costs associated with monetary charges, assessments, fines and/or penalties levied by a financial institution, credit/debit card company, credit/debit card processor from a data breach.

# Insurance Issues

---

- Application issues
- Liability and regulatory coverage
- Scope of “damages”
- Causation and measurement– data asset recovery and business interruption
- Retroactive and notice dates
- Consent issues (defense, forensics, settlements, etc.)
- Other insurance
- Other issues
- Remember - language varies; scope of coverage varies

# Final Thoughts

---

- Increasing sophistication of cyber attacks
  - State sponsored attack groups
  - Zero day vulnerabilities
  - Supply chain vulnerabilities
- Role of Insurers as partners for better data security and practices
  - Self-assessments
  - Table stakes data security for underwriting standards
  - Vendor vetting
  - Aggregation of event data
- Evolving threats, market forces, and coverage litigation will all affect cyber policies

# Questions?

---

**Jim Gallery**

Underwriter, US Cyber & Tech | Cyber Risks  
Beazley Group  
M +1 (773) 383 6099  
[Jim.Gallery@beazley.com](mailto:Jim.Gallery@beazley.com)

**Tim Jacobs CIPP/US**

Claims Manager – Cyber & Technology | Group Claims  
Beazley Insurance Services  
T +1 (312) 476-6266  
[Tim.jacobs@beazley.com](mailto:Tim.jacobs@beazley.com)





Thank you!