NACUA

Webinar

Sponsored by

LAWVU

2025 Cybersecurity Law Update

Kevin Dolan, Partner & Co-Chair, Advisory Compliance, Mullen Coughlin

Sajjad Matin, Principal Counsel, Cybersecurity and Data Protection, University of California

Agenda

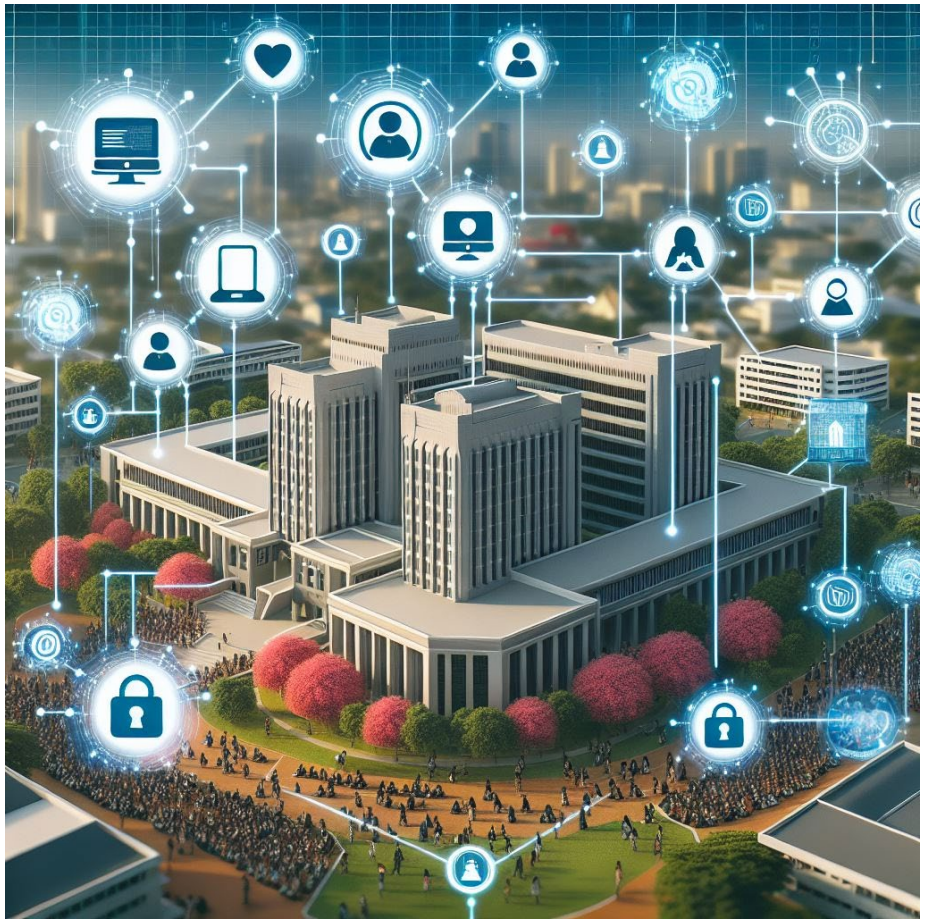
I. Welcome & Introduction
II. Overview of Cyber Threat Landscape
III. Compliance Framework
IV. Q&A
V. Practical Cybersecurity Challenges for Higher Education
VI. Q&A
VII. Concluding Remarks

Overview of Cyber Threat Landscape

NACUA

Unique Cyber Challenges for Higher Education

- Large Attack Surface
- Third-Party Vendor Risk
- Resource Constraints
- High Turnover
- Legacy IT Systems
- ***Valuable Data***



Valuable Data

Campus

Student Records

Title IV/PPA, GLBA – retention of student financial data

Research

Intellectual Property, Controlled Unclassified Info

Grants/Funding terms require retention of research data

Medical Center

Medical Records

HIPAA - retention of compliance documentation; State law - retention of medical records

Threats

Malicious attack

- **Hackers** in network; **malware** and viruses; **phishing scams** (ransomware); physical **theft** of hardware and paper

Employees

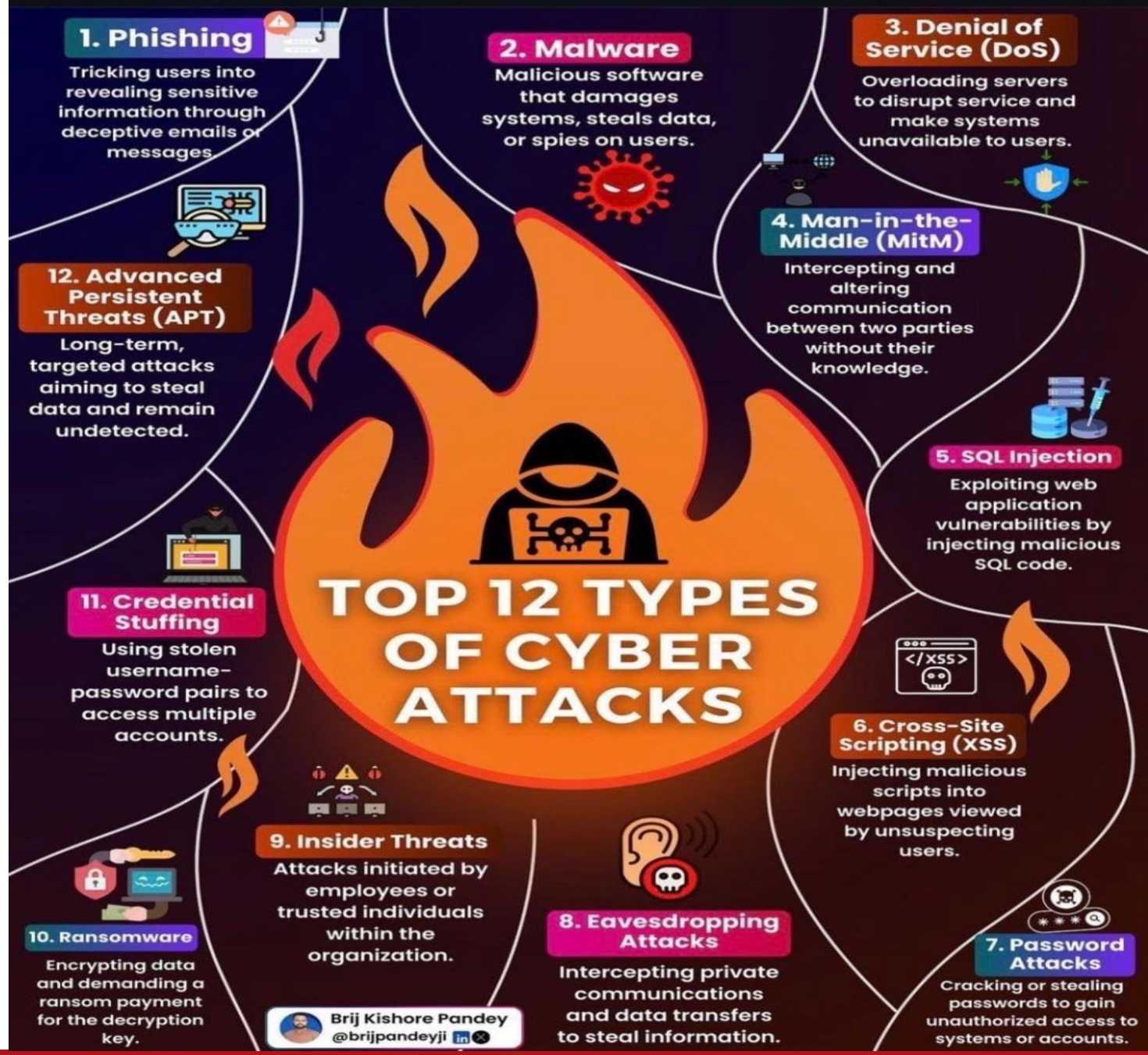
- **Rogue** employees
- **Negligence** related to the use and storage of data; failure to follow or learn policies and procedures; loss of portable devices; mis-mailing of **paper**; and/or unencrypted emails to the **wrong recipient(s)**

Business Partners

- **Any of the above** can occur to a business partner with whom data is shared

Supply Chain

- Event impacting **critical applications, software or infrastructure** utilized by organizations



Current Case Trends

- **Ransomware**
  - Triple Extortion/Harassment
- **Business Email Compromise**
  - Wire Fraud/Personal Information Harvesting
- **Software Exploits or Vulnerabilities**
  - Appliance & Application Zero-Days – *e.g.*, Cisco, SolarWinds, Fortinet
  - CISA Known Exploited Vulnerability Catalog
- **Third-Party Vendor Event**
  - MOVEit, Change Healthcare, PowerSchool

Artificial Intelligence & Cybersecurity

- AI-Enabled Social Engineering
- AI-Enhanced Cybersecurity Attacks
- Exposure or Theft of Vast Amounts of Nonpublic Information
- Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies

Incident Type

2021

Incident Type	Count
Ransomware	1,153 (29%)
Business Email Compromise (BEC) – Total	1,059 (27%)
BEC – Other	698
BEC – Wire Fraud	361
Third-Party Breach	623 (16%)
Network Intrusion	559 (14%)
Other	367 (9%)
Inadvertent Disclosure	209 (5%)
Total	**3,970 (100%)**

2022

Incident Type	Count
Business Email Compromise (BEC) – Total	1,077 (36%)
BEC – Other	733
BEC – Wire Fraud	344
Ransomware	732 (25%)
Network Intrusion	382 (13%)
Third-Party Breach	316 (11%)
Other	245 (8%)
Inadvertent Disclosure	207 (7%)
Total	**2,959 (100%)**

2023

Incident Type	Count
Business Email Compromise (BEC) – Total	1,343 (34%)
BEC – Other	996
BEC – Wire Fraud	347
Ransomware	884 (23%)
Third-Party Breach	749 (19%)
Other	403 (10%)
Network Intrusion	323 (8%)
Inadvertent Disclosure	218 (6%)
Total	**3,920 (100%)**

2024

Incident Type	Count
Business Email Compromise (BEC) – Total	1,601 (38%)
BEC – Other	1,224
BEC – Wire Fraud	377
Ransomware	1,011 (24%)
Vendor Breach	747 (18%)
Other	346 (8%)
Network Intrusion	322 (7%)
Inadvertent Disclosure	228 (5%)
Total	**4,255 (100%)**

Industry Sector

2021

Industry Sector	Count
Professional Services	1,024 (26%)
Manufacturing and Distribution	704 (18%)
Healthcare and Life Sciences	520 (13%)
Financial Services	461 (12%)
Technology	372 (9%)
Education	215 (5%)
Non-Profit	205 (5%)
Government	200 (5%)
Hospitality and Entertainment	152 (4%)
Retail/e-Commerce	73 (2%)
Energy	37 (1%)
Other	7 (<1%)
Total	**3,970 (100%)**

2022

Industry Sector	Count
Professional Services	773 (26%)
Manufacturing and Distribution	448 (15%)
Healthcare and Life Sciences	376 (13%)
Financial Services	350 (12%)
Technology	333 (11%)
Non-Profit	157 (5%)
Education	142 (5%)
Hospitality and Entertainment	139 (5%)
Government	122 (4%)
Retail/e-Commerce	84 (3%)
Energy	34 (1%)
Other	1 (<1%)
Total	**2,959 (100%)**

2023

Industry Sector	Count
Professional Services	928 (24%)
Financial Services	588 (15%)
Healthcare and Life Sciences	572 (15%)
Manufacturing and Distribution	538 (14%)
Technology	372 (9%)
Education	245 (6%)
Non-Profit	208 (5%)
Hospitality and Entertainment	169 (4%)
Government	138 (4%)
Retail/e-Commerce	130 (3%)
Energy	32 (1%)
Other	0 (0%)
Total	**3,920 (100%)**

2024

Industry Sector	Count
Professional Services	1,241 (29%)
Healthcare and Life Sciences	656 (15%)
Manufacturing and Distribution	563 (13%)
Financial Services	488 (11%)
Technology	342 (8%)
Education	241 (6%)
Non-Profit	212 (5%)
Hospitality and Entertainment	194 (5%)
Government	155 (4%)
Retail/e-Commerce	112 (3%)
Energy	51 (1%)
Other	0 (0%)
Total	**4,255 (100%)**

Ransomware Incidents

2021	
Number of RW Incidents	1,153 (29%)
Number of RW Incidents Paid	314 (27%)
Ransom Payment Reason	Delete Only – 44 (14%) Key and Delete – 150 (48%) Key Only – 120 (38%)
Average Ransom Demand	$2,126,671
Average Ransom Payment	$500,951
Median Ransom Payment	$216,093

2022	
Number of RW Incidents	732 (25%)
Number of RW Incidents Paid	97 (13%)
Ransom Payment Reason	Delete Only – 21 (22%) Key and Delete – 39 (40%) Key Only – 37 (38%)
Average Ransom Demand	$2,272,682
Average Ransom Payment	$400,791
Median Ransom Payment	$150,000

2023	
Number of RW Incidents	884 (23%)
Number of RW Incidents Paid	138 (16%)
Ransom Payment Reason	Delete Only – 42 (30%) Key and Delete – 56 (41%) Key Only – 40 (29%)
Average Ransom Demand	$2,243,227
Average Ransom Payment	$937,751
Median Ransom Payment	$200,000

2024	
Number of RW Incidents	1,011 (24%)
Number of RW Incidents Paid	133 (13%)
Average Ransom Demand	$1,890,232
Average Ransom Payment	$519,395
Median Ransom Payment	$265,065
Ransom Payment Reason	Delete Only – 53 (40%) Key and Delete – 49 (37%) Key Only – 31 (23%)

Ransomware Risks and Considerations

Legal Considerations

- ❑ Can we confirm that the threat actor is not linked to a sanctioned entity (will the payment/negotiation vendor provide a clear sanctions report)?
- ❑ Has there been timely and cooperative involvement with law enforcement?

Ransomware Risks and Considerations

Operational Considerations

- Are critical data/systems fully or partially recoverable without the decryption key, i.e., will any data loss occur?
- What is the value of lost data and the risks of lost data from an operational perspective?
- What is your recovery timeline?
- Are funds available for payment? Consider funds necessary for other costs relating to recovery from the incident (legal, forensic investigation, notification, third party claims).
- What role does the insurance carrier have in the payment and negotiation process?
  - Have their required processes been filed?
  - Will the insurance carrier issue the funds for the ransomware payment directly to the negotiations team or is organization responsible for the costs and submit for reimbursement?
- Who internally needs to approve the ransomware payment and what information do they need to reach this decision?

Ransomware Risks and Considerations

Reputational Considerations

- Does the exfiltrated data include sensitive proprietary or personal information? How do we quantify the value of potential harm of data being published?
- If data exfiltration occurred, does the value of suppressing the data theft justify the cost of the key even if the key is not necessary for decryption purposes?
- What is the reputational cost of operational downtime?
- If the ransom payment becomes public knowledge, will there be a reputational, liability, and/or regulatory cost associated with paying the ransom?

Lawyer's Role in Incident Response

- Collaborate with Incident Response Team to identify:
  - Scope/impact of incident
  - Sensitive data or systems impacted
- Vendor breach – review contracts
  - Indemnification/LOL
  - Notification requirements
- Research Data – contracts/grants from funding sources
  - Notification terms
  - Terms related to Cybersecurity Controls (ACP)

Guidance on Attorney Client Privilege - *Provided to InfoSec Colleagues*

1. The goal is to protect against disclosure (in later litigation) of sensitive legal discussions.
2. Attorney-Client Privilege protects:
   - **Internal** Communications;
   - With a lawyer; and
   - Seeking/Receiving legal advice.
3. Operational communications typically will not be protected under ACP.
4. Communications without a lawyer present will not be protected.
5. Local counsel is often a member of IRT, keep counsel in the loop (on all threads).

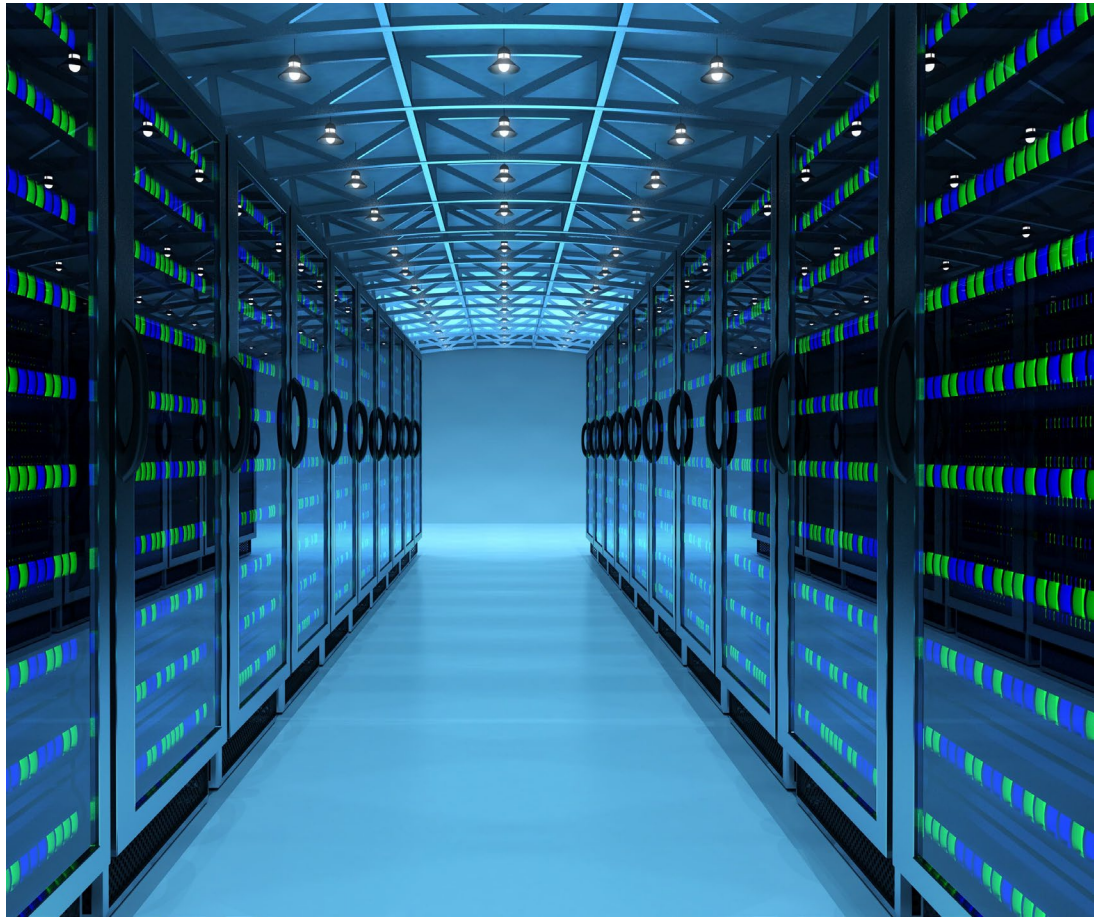
Privilege During a Cyber Incident

- Legal Advice vs. Operational Guidance
- If needed, outside counsel should retain SME/forensic firm
  - Separate engagement for Legal vs. InfoSec
  - Separate, privileged report for Legal
- Disclosure of Reports to Law Enforcement
  - Federal Rules of Evidence - 502 – potential waiver of other documents relating to subject matter
  - GJ subpoena – documents may be Brady/Giglio

Investigation Directed by Counsel

Create guidelines for when counsel takes over investigation:

1. Who makes the decision (e.g., President/Chancellor)?
2. What factors will be used?
   - ✓ Whether data was exfiltrated
   - ✓ Type of data impacted
   - ✓ Number of records impacted
   - ✓ Reputational harm



Cybersecurity Compliance Framework

NACUA

State Regulatory Exposure

- **50 states** (plus Puerto Rico, Washington D.C., the Virgin Islands and Guam) require notice to residents after unauthorized access to personally identifiable information (PII)
- Require companies to **notify resident consumers** of security breaches of unencrypted computerized personal information
- Over half require **notification to state attorney general**, state consumer protection agencies, and/or consumer reporting agencies
- Some states allow **private right of action** for violations

State Legislative Trends

- Expanding the definitions of “personal information” (*e.g.*, including biometric information, email address w/password, passport number, etc.)
- Set a timeframe/shorten timeframe within which businesses must report a breach
- Require reporting of breaches to state attorney general
- Sector specific laws requiring data breach notification (e.g., education/student data vendors)
- A few states provide affirmative defense for data breaches if organization implements proactive industry recognized information security standards
- More states are becoming active in data privacy regulation and enforcement

Privacy Regulation Trends

Emerging state level patchwork

- What applies to us?
- Which types of data are afforded protection?
- Enforcement

Federal Frameworks

- FTC
  - Sources of authority
    - **Section 5 of FTC Act**
    - GLBA
    - Children's Online Privacy Protection Act
    - Fair Credit Reporting Act
- SEC Cybersecurity Rule
- HIPAA

Digital Risk Management

Function:

Identifying, assessing, and mitigating risks associated with digital infrastructure that impact data and IT systems that process it.

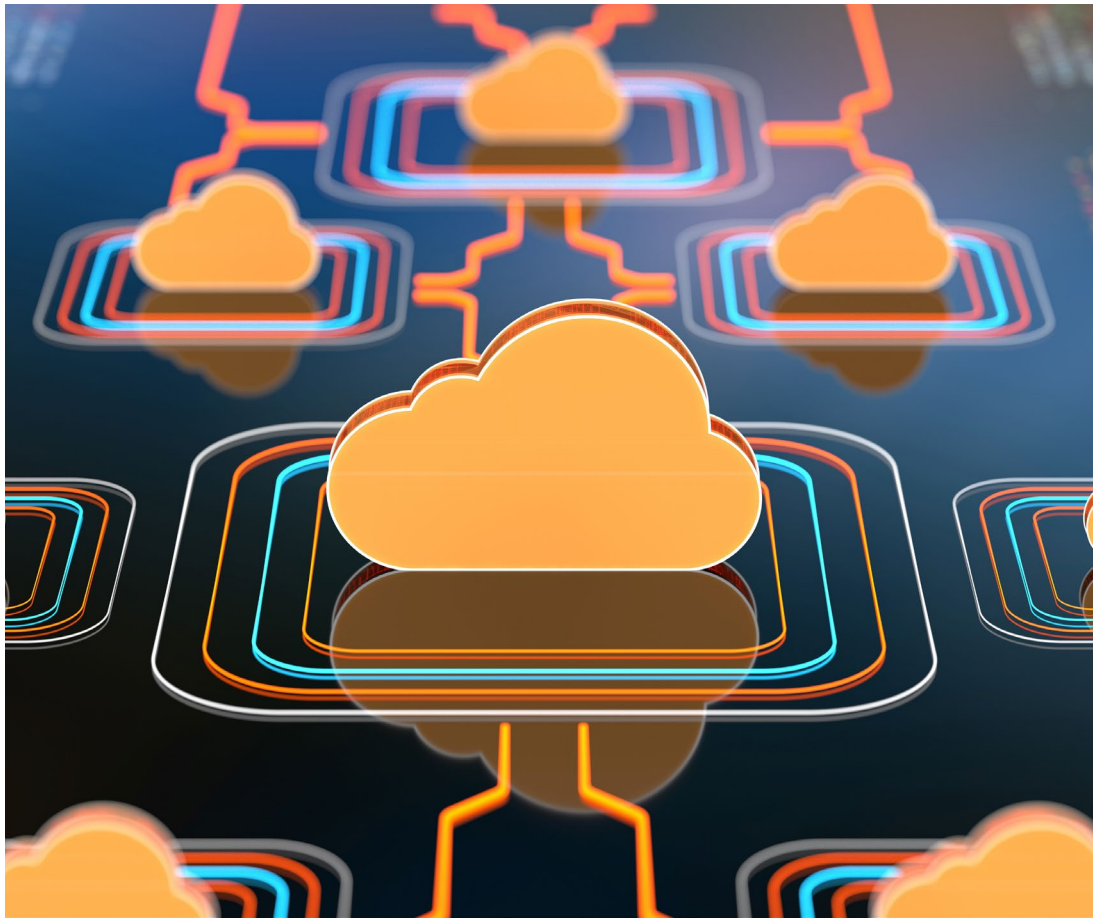
Goals:

- Data Protection (***Cybersecurity*** + Data Privacy)
- Compliance with legal/regulatory requirements
- Manage third-party risks (including vendors, law firms, unions)
- Establish roles and responsibilities

Important Cybersecurity KPIs for Lawyers

- Cybersecurity Training Completion Rate
- Phishing Test Success Rate
- Percentage of accounts behind MFA
- Vulnerability Patch Time/Percentage of Assets Unpatched
- **Vendor Compliance Rate**
- Incident Metrics: Mean time to Detect, Mean time to Respond
- Cost per Incident; Cost per Breach

Vendor Risk Assessment

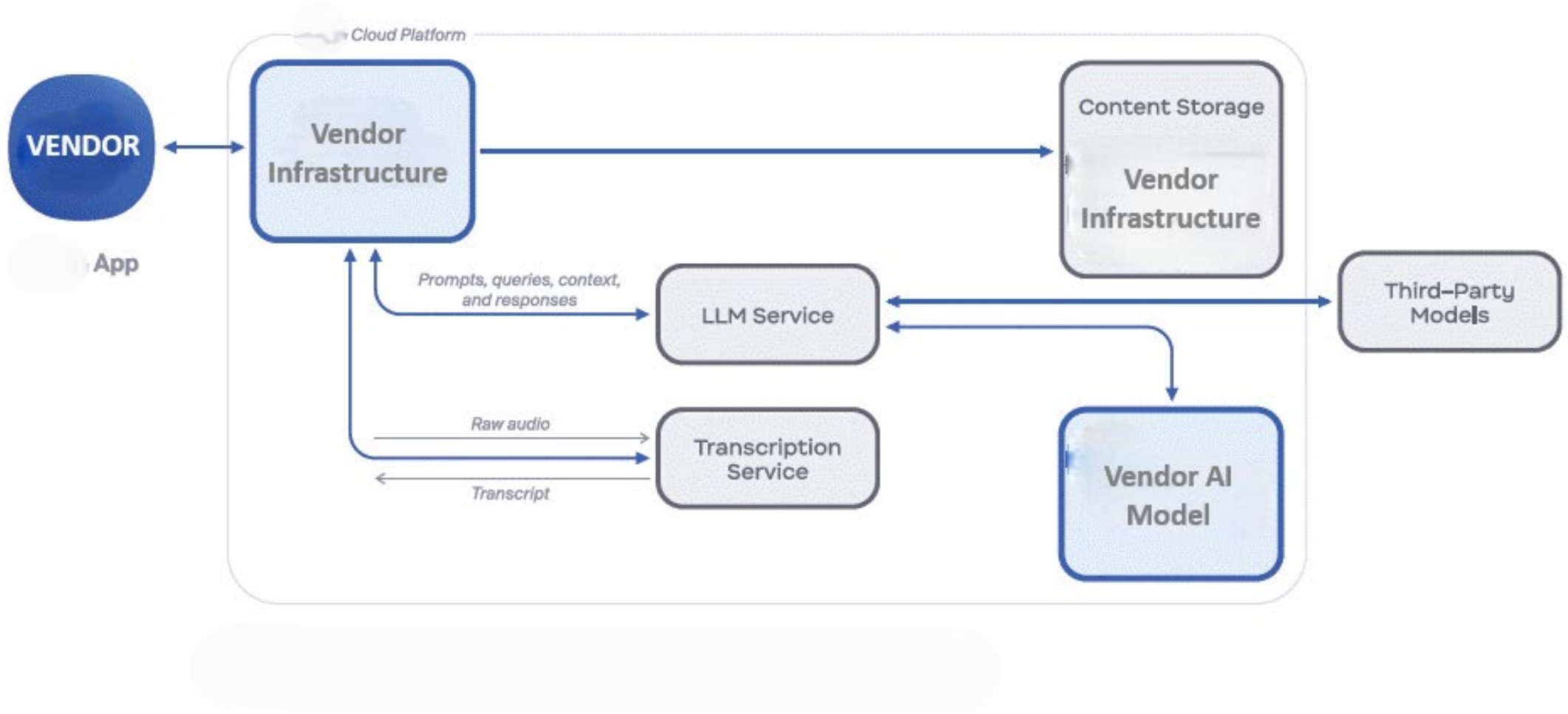


- How is customer data processed?
- How is customer data is used:
  Product Improvement?
  Training/tuning/feedback for AI models?
- Security Controls
- Incident Response
- Business Continuity
- Reputation and Track Record

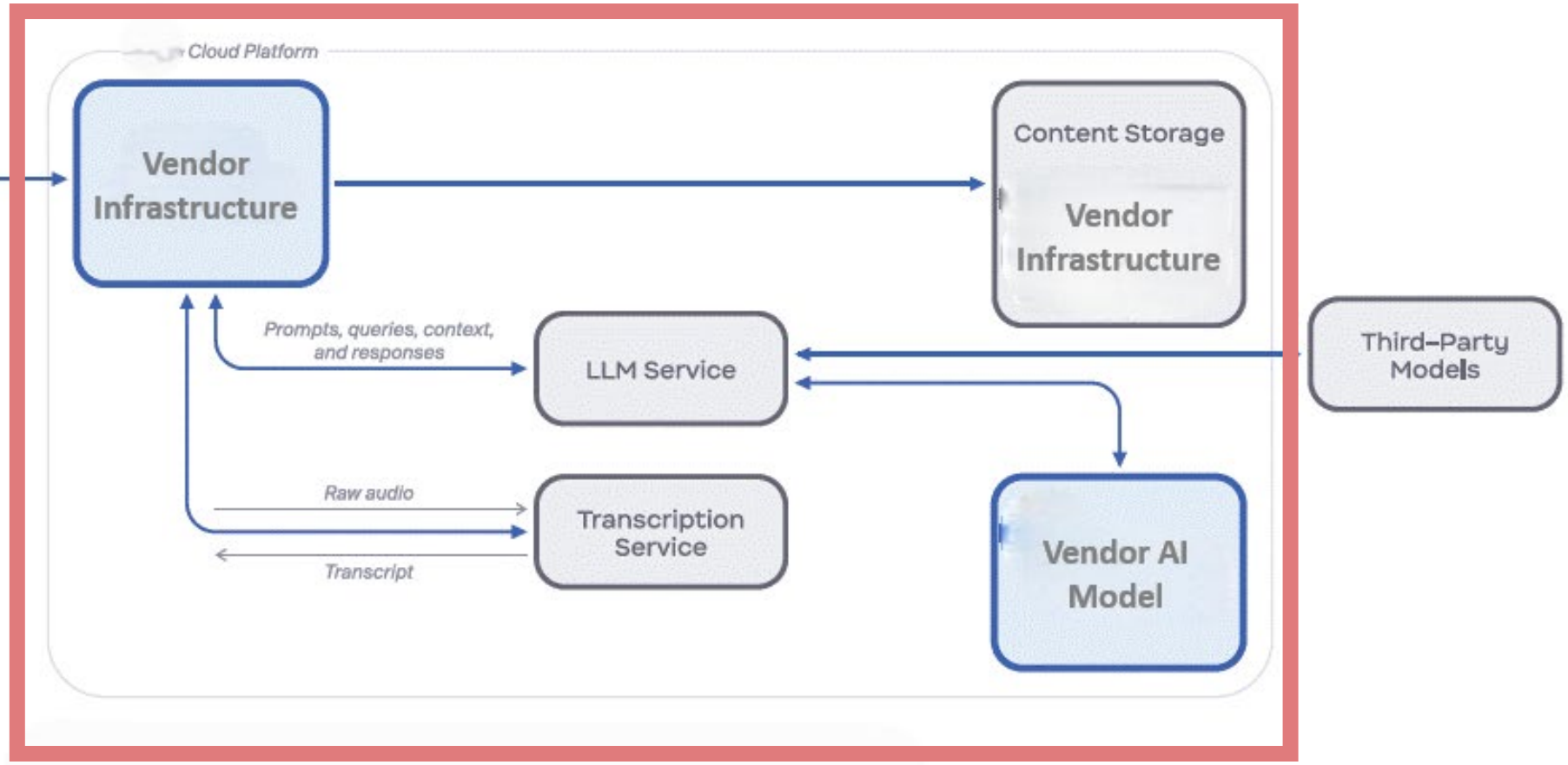
Leverage VRA for Contract Negotiation

- Can you minimize data processed by vendor; Can you minimize data retention by vendor?
- Is “Customer Data” appropriately defined?
- Security Breach Indemnification
- Limitations of Liability
- Cyber Insurance

Vendor Risk Assessment – AI Example

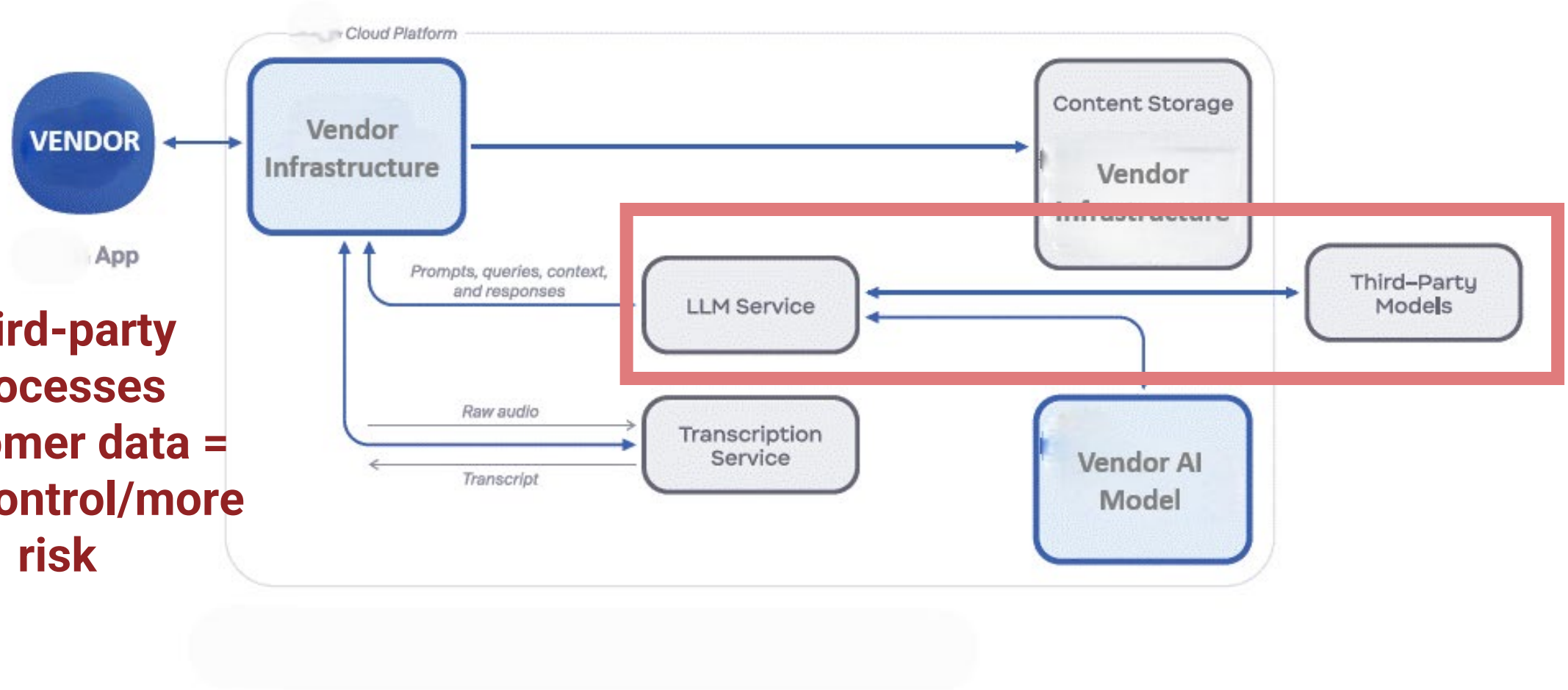


Vendor Risk Assessment – AI Example



Vendor retains control of data

Vendor Risk Assessment – AI Example



Third-party processes customer data = less control/more risk

Practical Cybersecurity Challenges

NACUA

Understanding the Stressors Affecting the CISO

- Expanding Role/Increasing Responsibilities
- Increasing Legal Risk (Perceived and Real)
- Increasing Demands from Campus Stakeholders
- Blame following a Breach

Statements/Attestations by CISOs

- Regulatory Compliance (HIPAA, GLBA, FSA, PCI DSS)
- Contractual Agreements (e.g., procurement, handling research data)
- Internal Governance and Risk Management
- Third-Party Assessments
- Other (e.g., bond disclosures)

CISO – Legal Risk

In October 2021, DOJ announced the "Civil Cyber-Fraud Initiative“

The stated goal "to hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, ***knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches***."

CISO – Legal Risk (Criminal)

United States v. Sullivan

No. 3:20-cr-00337-WHO (N.D. Cal. Jan. 11, 2023)

- Joseph Sullivan was the Chief Security Officer for Uber.
- In November 2016, Uber's systems were hacked.
- Sullivan's actions in response to that cyber incident resulted in his prosecution for and conviction of obstruction of justice and misprision of a felony.
- He was sentenced to 3 years' probation in December 2023.

CISO – Legal Risk (Civil)

SEC v. SolarWinds and Brown

No. 23-civ-9518 (S.D.N.Y. filed Oct. 30, 2023)

- Timothy Brown was the CISO of SolarWinds.
- SolarWinds is a provider of IT infrastructure management software.
- Its products were subject to sophisticated cyberattack and intrusion over a two-year period (SUNBURST).
- The SEC claims the company and CISO made misleading cybersecurity disclosures in the company's Security Statement.

CISO – Legal Risk

United States ex rel. Decker v. Pennsylvania State University
No. 2:22-cv-03895 (E.D. Pa.)

- Whistleblower, former CIO for Penn State's Applied Research Lab, alleged university non-compliance with contractual cybersecurity requirements for federal funding of research.
- The university settled with DOJ for $1.25M in October 2024.
- The allegations in the complaint also named other information security officers who purportedly directed or approved inaccurate representations to the government.

CISO – Legal Risk

United States ex rel. Craig & Koza v. Georgia Tech Research Corp.

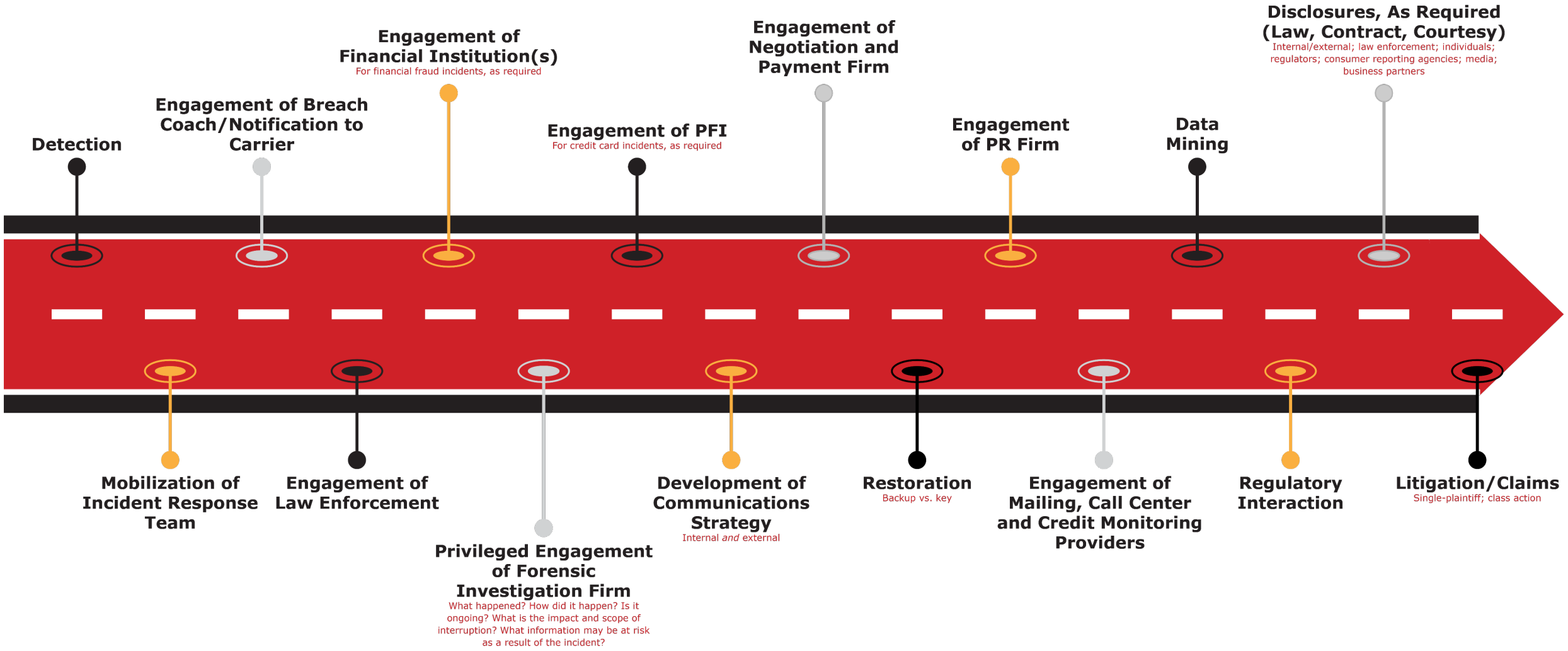
No. 1:24-cv-01234 (N.D. Ga. Apr. 15, 2024)

- Whistleblowers, one current and one former infosec officer within GA Tech, alleged, among other claims, non-compliance with contractual cybersecurity requirements for federal funding of research.
- In August 2024, DOJ intervened in the suit.
- The allegations in the complaint also reference other staff and faculty who purportedly directed or approved non-compliant IT settings.

Take-Aways for CISOs

1. Criminal prosecution for decision-making that involves highly technical matters is *RARE*. Why?
   - Battle of the Experts
   - Confusing a jury with technical matters
   - Reliance of Counsel Defense (Affirmative Defense)
     - requires “full disclosure of all material facts” (Ninth Cir. Jury Instructions)
2. Communication to Partners (including Legal)
   - Early and Often
   - Don’t “hope away” bad facts
   - ELI5

The (Potential) IR Roadmap




Questions?

NACUA materials, PowerPoint slides and recordings available as part of this program are offered as educational materials for higher education lawyers and administrators. They are prepared by presenters and are not reviewed for legal content by NACUA. They express the legal opinions and interpretations of the authors.

Answers to legal questions often depend on specific facts, and state and local laws, as well as institutional policies and practices. The materials, PowerPoint slides and comments of the presenters should not be used as legal advice. Any hypothetical scenarios presented are based on fictional facts and persons. Legal questions should be directed to institutional legal counsel.

Those wishing to re-use the materials, PowerPoint slides or recordings should contact NACUA (nacua@nacua.org) prior to any re-use.