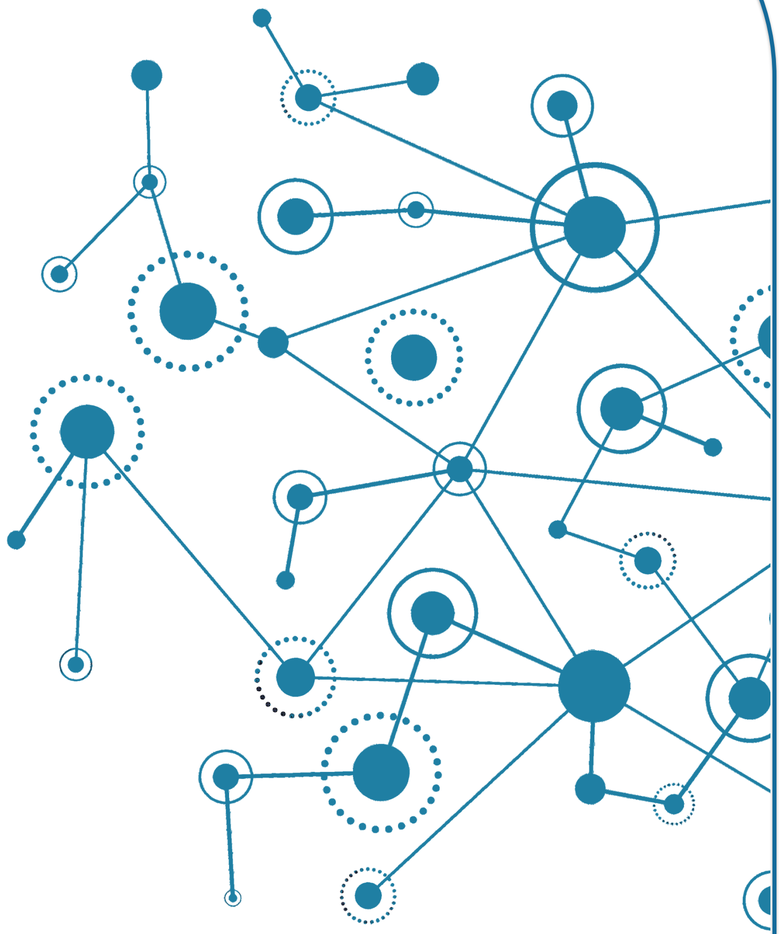
DOCENT | studios

CornCon 11

Manifest your inner Cyber Superhero



Privacy, Privilege, and Proactive Response: Legal Strategies for Cybersecurity Excellence

October 10, 2025
CornCon Cybersecurity Conference

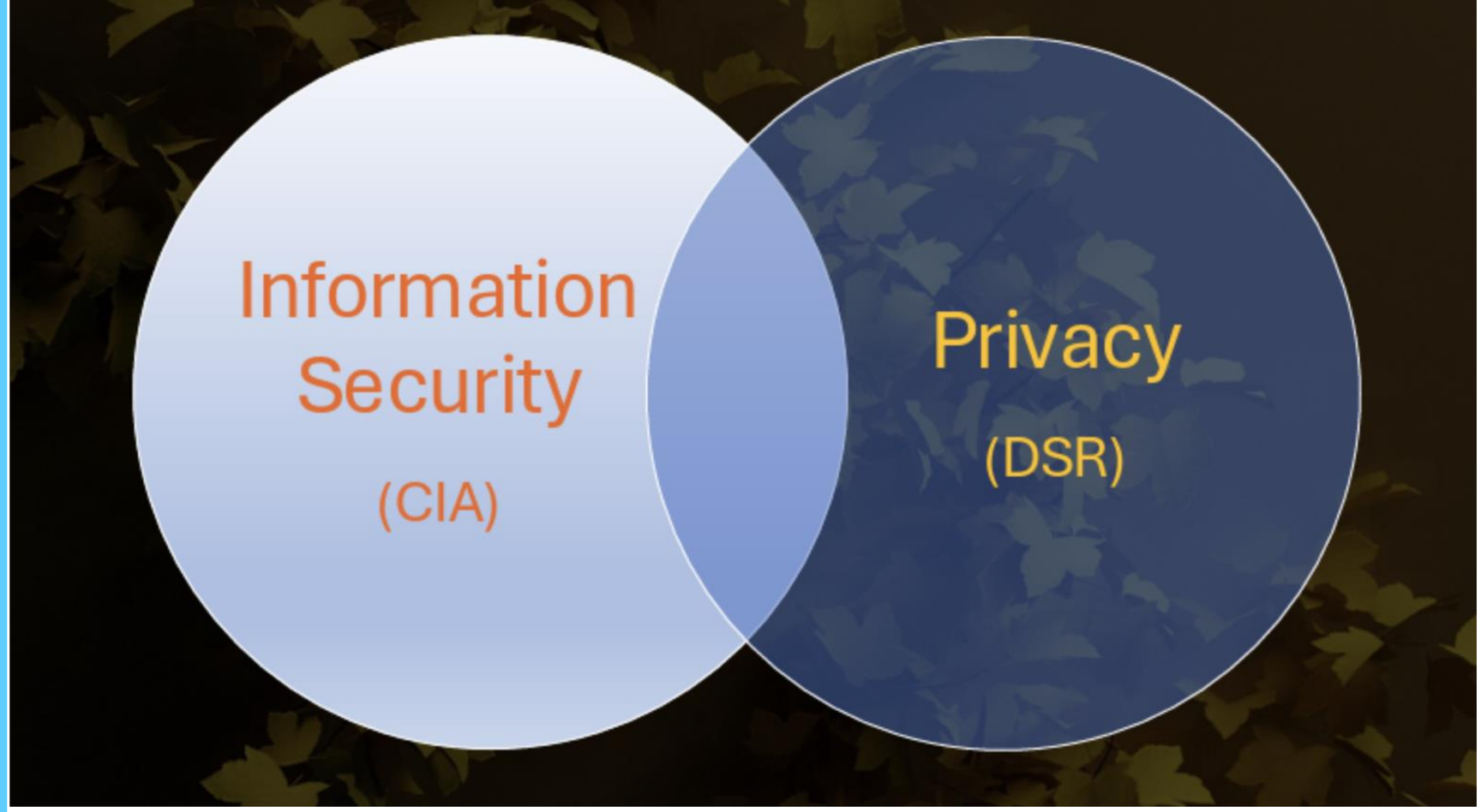
Paul Rice

Sr. Legal Counsel
PayPal Inc.

Disclaimers

- IANYL
- Not legal advice, these are my personal opinions and not those of my employer
- When in doubt, Consult Your Attorney (CYA)

Why 'cybersecurity excellence' requires information security legal risk management



The triad:

- Legal Basis for Information Governance
- Preserving Privilege During Incident Response
- Proactive Incident Response Planning

Legal Basis for Information Governance as part of Operational Risk

Non-exhaustive

- U.S. State and Federal: CCPA/CPRA, state reasonable security statutes, state breach notification statutes, sectoral laws (HIPAA, GLBA, FERPA, etc.)
- GDPR: breach notification (72 hrs.), security of processing (Art. 32), cross-border transfers
- International: NIS2 Directive, DORA, Canada's PIPEDA, Brazil's LGPD

Governance, Risk, and Compliance (GRC) Integration

Cybersecurity Legal Team as an Enterprise Risk Partner

- Collaborating with business units: CISOs, Compliance, HR, Finance, and Communications
- Legal's role in board and regulator engagement

Preserving Privilege During Incident Response

What is Legal Privilege

Provides for openness and efficiency when seeking legal advice and counsel

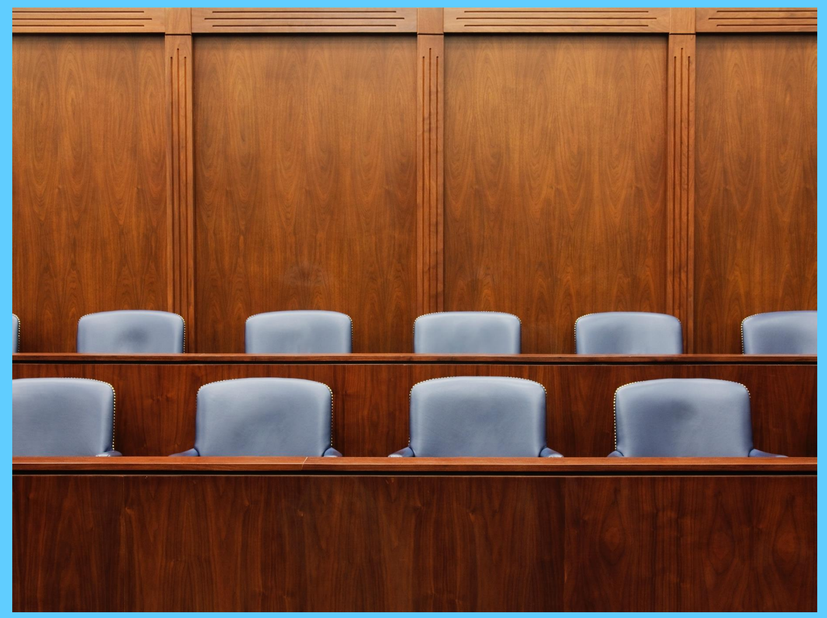
Attorney-Client Privilege

- Protects communications between attorney and client made for the purpose of seeking or providing legal advice
- Client must intend the communication to be confidential, and privilege can be waived

Work Product Doctrine

- Protects materials prepared by attorneys in anticipation of litigation from discovery by opposing parties
- Covers attorney notes, research, strategy documents, and mental impressions about the case
- Provides qualified protection that can be overcome in limited circumstances with sufficient showing of need

Why Privilege Matters



- Discovery risks in litigation and regulatory investigations
- Privilege does not protect underlying facts, only the confidential communications about those facts
- Vested with the client (the organization), but enhanced by all

Practical Mechanisms

Tips to Establish and Preserve Privilege

- Labeling & Segregation – privileged and confidential, prepared at the request of counsel
- Retaining outside counsel as first line of engagement
- Ensuring forensic reports are directed to and controlled by counsel
- Drafting communications as legal advice, not business updates

Pitfalls and Case Law Lessons Regarding Thinning Privilege

- Instances where courts pierced privilege (overly broad distribution, lack of legal purpose)
- What successful privilege assertions looked like

Proactive Incident Response & Preparedness

Incident Response Planning

- Legal’s role in developing and approving the IR plan
- Escalation ladders for counsel involvement
- Embedding legal decision points
  - forensics/fact gathering
  - breach determination
  - regulatory thresholds
  - Obtaining outside assistance under privilege
- Designating 'legal champions' for IR readiness
- Tactics, Techniques, and Procedure (TPP) sharing
- Crisis communication oversight (e.g., press, customers, partners, board, regulators)

Tabletop Exercises

- Scenario planning for ransom payments, insider threats, vendor incident, or operational
- Integrating privilege into exercises
- Cross-functional role clarity for business units (IT, Legal, Compliance, Comms, Risk, Treasury, HR)

Incident Response Regulatory & Contractual Reporting Obligations*

*(A non-exhaustive discussion of considerations, because others get a vote as well)

Legally Required Breach Notification Considerations

Consult Your Attorney

- Incident vs. formal declaration of a “Breach”
- Categories of information accessed or exfiltrated
- Risk of harm standards
- For some companies:
  - Legal standards for 'material' incidents (SEC guidance, 8K type 1.05 vs general disclosures, case law)
  - Sectoral reporting obligations (Broker-Dealers, Banks, Critical Infrastructure)
  - Waterfall provisions (NYDFS, RI, Australia)

Contractual Considerations

Consult Your (Transactional) Attorney

- Notification triggers and reporting timelines
- Cyber insurance notification clauses
- Contractual flow-downs
- Creating a defensible paper trail

Legal Incident Response Playbooks

- Notification guidance and regulatory engagement strategies
  - Courtesy vs. actual notice, prior corporate practices, upcoming exams
  - "At this time" "As part of our ongoing investigation" "Currently" "We believe"
  - May include pre-drafted holding statements or form examples (e.g., NYDFS, GDPR SA)
- Considerations beyond legally required disclosures

Post-Incident Privileged Review

Post-Incident Privileged Review

(aka Now What?)

Structuring the Post-Mortem

- Ensuring remediation discussions remain privileged
- Balancing transparency with litigation/regulatory posture

Continuous Improvement

- Lessons learned embedded into IR plan updates
- Regulatory and litigation long tails
- Using findings for compliance reporting (FTC orders, SEC undertakings)

Building Resilience

- Strengthening vendor and contractual oversight
- Enhancing training and awareness for legal and business teams

Key Takeaways & Action Steps

Information Security Legal Strategy Isn't Just Defense—It's a Core Enabler of Trust and Resilience

- Legal Basis for Information Governance: Ongoing compliance is foundational to cybersecurity excellence
- Preserving Privilege During Incident Response: Counsel must proactively structure and help
- Proactive Response: Legal should play a role with planning, reporting, and continuous improvement

Bonus Content - Incident Response Tear Sheet - Legal Counsel Considerations in NIST Incident Response Model

Legal Counsel Considerations in NIST Incident Response Model

I. Preparation

- Privilege Framework
  - Structure forensic/consultant engagements through counsel to preserve privilege.
  - Establish protocols distinguishing between "business" and "legal" reports.
  - Preserving evidence and overseeing investigation
- Contracts & Insurance
  - Obtain awareness for the process to review and track vendor/customer contracts for incident notice obligations.
  - Craft language to require notice only with "confirmed" impact to the Vendor's information or services provided.
  - Confirm insurance reporting requirements and panel counsel rules.
- Refine Outside Counsel Mapping
  - Maintain a roster of regional outside counsel with breach/IR expertise for rapid engagement.
- Incident Response Champions
  - Designate champions within the legal team to own readiness and reporting.
  - Ensure champions document a factual basis to support legal analysis in incident determinations and post incident reviews.

II. Detection & Analysis

- Determination of "Breach"
  - Advise on whether an incident has crossed into "breach" territory under specific statutes (e.g., unauthorized access vs. unauthorized acquisition).
  - Document legal reasoning for materiality assessments (especially for SEC 8K).
- Privilege Shielding
  - Direct team members to funnel comms through counsel.
  - Mark contemporaneous documentation as prepared at counsel's direction.
- Regulatory Impact Assessment
  - Quickly identify potential reporting obligations by data type and jurisdiction.
  - Consider law enforcement implications (reporting vs. risk of waiving privilege or inviting scrutiny).
- Initial Briefings
  - Frame updates under privilege, avoiding speculative or technical overreach.

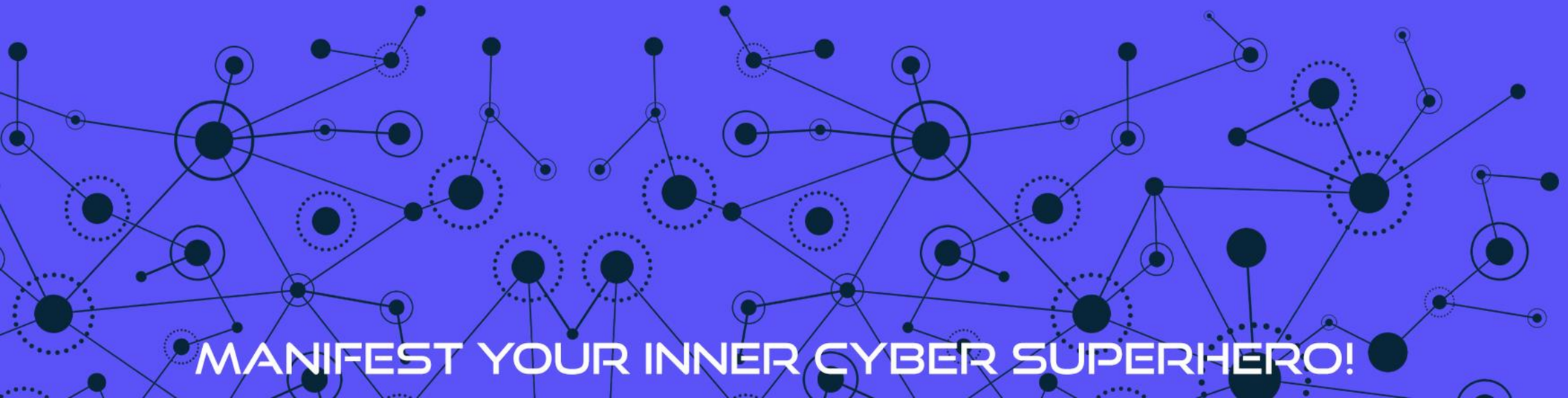
III. Containment, Eradication, and Recovery

- Notification Determinations
  - Apply statutory and contractual obligations against the evolving facts.
  - Document rationale for "notify vs. no notify" decisions under privilege.

Most Common Private Rights of Action in Recent Data Breach Litigation

- Common law: Negligence, implied contract, privacy torts frequently asserted for data security failures
- Class actions: Most breach claims pursued as class actions seeking monetary, injunctive, and declaratory relief.
- Circuit Splits: standing - Ongoing debate around whether future risk of identity theft qualifies for legal action

Thank You



MANIFEST YOUR INNER CYBER SUPERHERO!