October 3, 2024

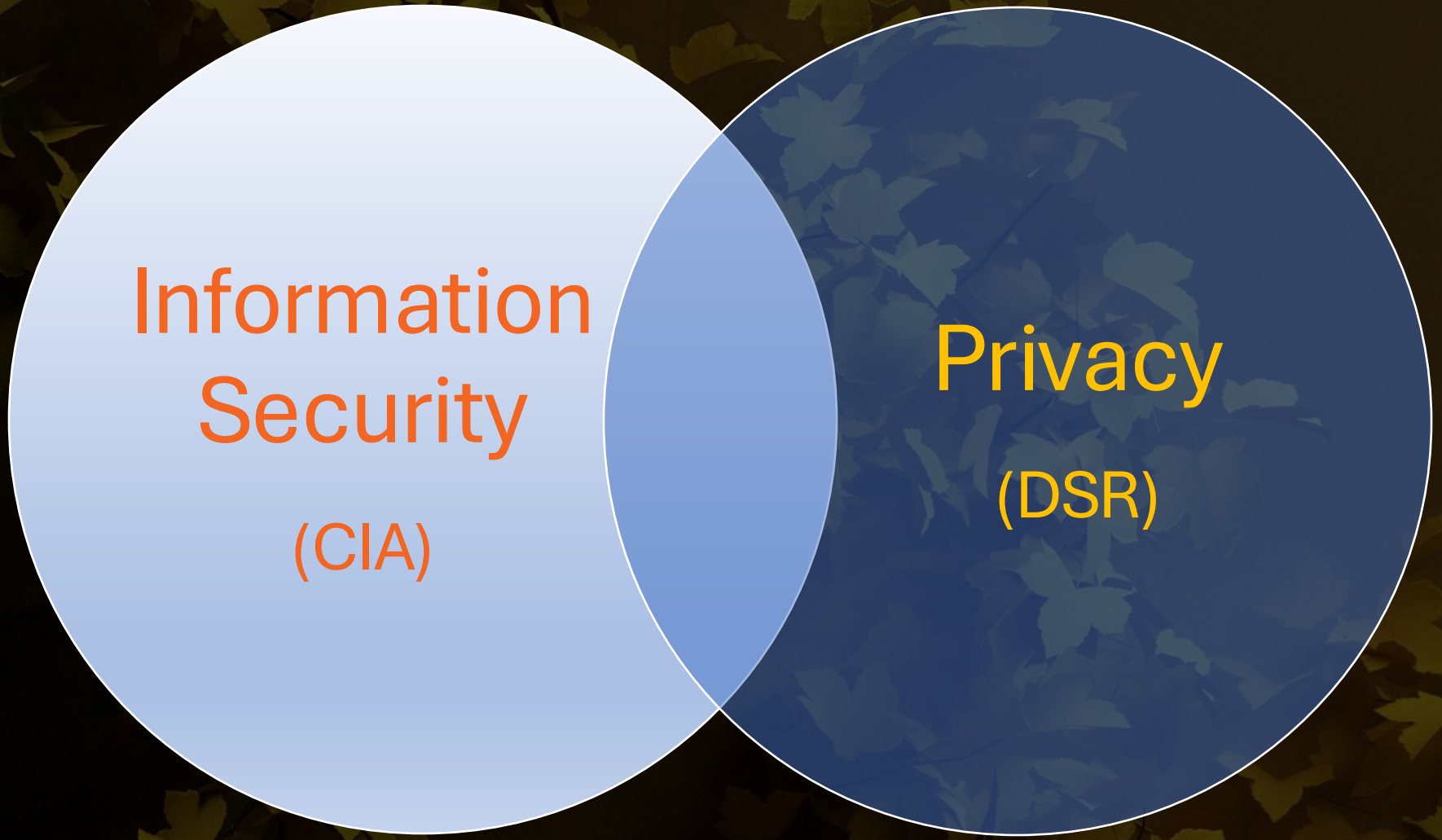
Update from the Trenches

Legal RPG – “It Depends”

Paul Rice

1. Introduction and Disclaimers
   - IANYL
   - Not legal advice, these are my personal opinions and not those of my employer
2. Discussing topics and trends based on supporting organizations from the trenches

Information Security and Privacy Law



Sources of Affirmative Requirements for “reasonable security”

Federal Sectoral Regulations

- Public Companies (SOX)
- FTC Section 5
- Government, Heath, or Financial Services

State Laws (CA, VA, & MS)

- ““Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data…””

State Data Breach Exceptions

- Use of encryption
- Governed by federal law

Europe (GDPR Art. 33 & NIS2)

Contractual (ToS, Contracts, and DPA)

Incident Response Considerations

1. Plans and preparation
2. Privilege
3. Outside Assistance
4. Containment, remediation, and communications
5. Breach notification analysis
6. Statutory notifications
7. Sector-specific rules
8. Long-term remediation
9. Lessons learned
10. Plan, prepare, test

Privilege

- Prong one: Establish (in writing and in practice) that Legal oversees the investigation in order to preserve privilege claims
- Prong Two: Consider the contents of written communications in case privilege is not upheld

Outside Assistance

- Insurance
  - Notification
  - Panel Providers
- Panel Providers
  - Tripartite agreements
  - Retainers
  - Resources
  - Validation
- Law Enforcement
  - Consultation
  - Assistance

Inputs to Notification Considerations (Zone of Impact)

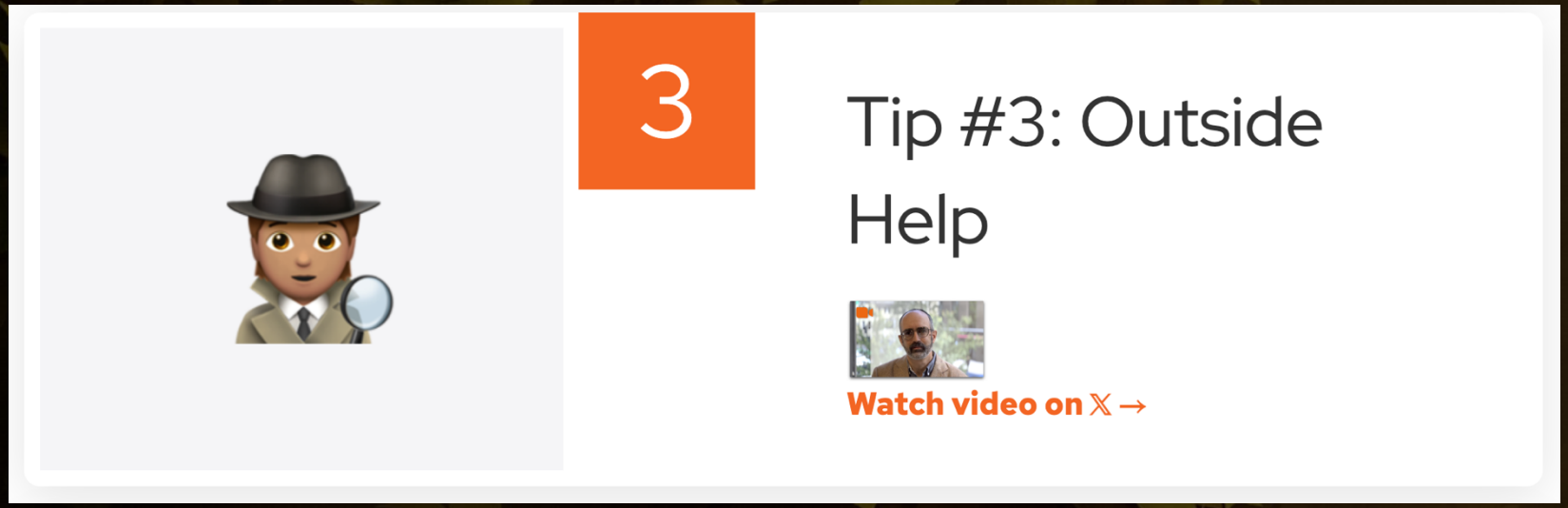
- Available evidence of access or download
- Jurisdiction
- Approximate number of individuals in each jurisdiction
- Categories of personal data

Information Supply Chain Attacks

- Indirect targeting (employees, vendors, and customers)
- Trust exploitation
- Lateral movement
- Data Exfiltration
- Accelerants and distractions

More resources

- https://www.zwillgen.com/cyber/



Ask me anything

Bonus Content

CA Proposed Risk & Cybersecurity Audit Regulations

- The CCPA created a duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, [so as] to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"

But what is "reasonable security?"

- On August 29, 2023, the California Privacy Protection Agency ("CPPA") Board issued draft regulations on Risk Assessment and Cybersecurity Audit. The CPPA Board discussed the Draft Regulations during a public meeting on September 8, 2023.

- The CPPA Board has started the formal rulemaking process for these two topics and the release of these Draft Regulations is (apparently) intended to facilitate Board and public discussion

CA Draft Risk Assessment Regulations

- Draft would require California businesses to assess their risks related to:
  1. "Selling" or "sharing" personal information
  2. Processing sensitive personal information
  3. Using "automated decision-making technology" to make certain consequential decisions
  4. Processing the personal information of consumers under 16
  5. Using technology to monitor employees, independent contractors, job applicants, or students
  6. Using technology to monitor consumers' behavior, location, movements, or actions in publicly accessible places
  7. Processing the personal information of consumers to train artificial intelligence or automated decision-making technology
- Expansive new definitions for "Artificial Intelligence" and "Automated Decision-Making Technology" with additional requirements for businesses that use these tools
- Would require documenting risks and associated safeguards, and updating assessments after each "material change" in processing activity
- Businesses would be required to submit risk assessments to the CPPA (in abridged form)

CA Draft Cybersecurity Audit Regulations

- The categories of businesses required to complete cybersecurity audits along with thresholds for each category
- New definitions, including Zero Trust
- Detailed requirements for conducting cybersecurity audits
- Requirements to submit a notice of compliance to the CPPA, including either:
    1. A written certification that the business has complied with the regulatory requirements during the 12-month period that the audit covers, or
    2. a written acknowledgement that the business did not fully comply with the regulatory requirements during the 12-month period the audit covers, identifying areas of noncompliance and providing a remediation timeline or confirmation that remediation has been completed.
- New contractual requirements compelling third parties to assist with business-performed compliance audits

What is the NIST Incident Response Framework?

- The National Institute of Standards and Technology (NIST) is an agency operated by the United States' Department of Commerce which provides standards and recommendations for many technology sectors.
- NIST ITL developed an influential model for incident response (IR), the Computer Security Incident Handling Guide (Special Publication 800-61).
- The NIST incident response process is a cyclical activity featuring ongoing learning and advancements to discover how to best protect the organization. It includes four main stages: preparation, detection/analysis, containment/eradication, and recovery.

NIST Process Diagram