American Public Transportation Association
Legal Affairs Seminar
February 26, 2018

Laws Governing Sensitive Information & Tips for Advising on Common Cyber Security Issues

Catherine Groves, Attorney

Phone: 415-995-5171

cgroves@hansonbridgett.com

Agenda

- Categories of Protected Information
- What's the Risk?
- Attorneys' Professional Conduct Obligations
- What is Data Security?
- How to Protect Yourself & Clients: Reasonable Security Controls
- Tips for Common Issues:
  - Software/SaaS (Cloud) Agreements
  - Preparing for and responding to a data security incident

Categories of Protected Information

- Personally Identifiable Information (PII)
- Payment Card Information (PCI)
- Protected Health Information (PHI) & Electronic PHI (EPHI)
- Miscellaneous
  - Automated License Plate Recognition Systems (Cal. Civil Code §§ 1798.90.5-1798.90.55, 1798.29, 1798.82)
  - Electronic Tolls & Electronic Transit Fare Collection (S&H Code § 31490)
  - **https://oag.ca.gov/privacy/privacy-laws**

What's the Risk?

- Types of Threats to Data Security & Privacy
  - Phishing
  - Physical Theft & Lost Media
  - Hacking
  - Ransomware
  - Malicious Software (Malware): Viruses, Worms, Trojans and Spyware
- What's "the Cloud" & How Does it Change Things?
  - SaaS versus traditional software
  - Consultants
  - More parties accessing data
  - Becoming ubiquitous
  - Significant legal risk associated with breaches

Attorneys' Obligations

- California Rules of Professional Conduct
  - Rule 3-100 (Duty of Confidentiality) & Rule 3-110 (Duty of Competence)
  - The California State Bar Formal Opinion 2010-179: Duty of confidentiality requires us to protect our clients secrets by maintaining good data security practices
- ABA Ethics:
  - Model Rules 1.1 and 1.6: Require attorneys to take competent and reasonable measures to safeguard information relating to clients.

What's Data Security?

Data Security is all about "CIA:"

- ***Confidentiality***: Access to Sensitive Data "limited to need to know."
- ***Integrity***: Data is protected from intentional or inadvertent changes while in transit or at rest.
- ***Availability***: Those authorized to access or use the data for legitimate purpose can do so when needed.

How to Protect Yourself & Clients: Implement Reasonable Security Controls

- PII: Cal. Attorney General Report
  - Center for Internet Security (CIS) Critical Security Controls (20)
  - Certification to ISO-27001 (114 controls in 14 groups and 35 control objectives)
- Cardholder Data: Payment Card Industry Data Security Standard (PCI-DSS)
- PHI/EPHI:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)

Common Issues: Software/SaaS Contracts

How sensitive is the data? How often do you need to access it? What happens if it disappears, is hacked, or the contractor cuts off access?

- Type of data – require reasonable security controls linked to specific standards & compliance representations
- Availability of data (uptime requirements) through service level agreement (SLA)
- Ownership and location of data (get regular back ups!)
- Transition & sharing data

Common Issues: Software / SaaS Contracts Cont.

- Hosting facility physical & internet security
- Disaster recovery and location of the primary and back up data centers
- Records retention, PRAs, subpoenas, disposition and legal/litigation holds
- Dispute Resolution/Venue
- Disabling Code
- Termination provisions and vendor bankruptcy
- Indemnification – including “security incident” and data breach
- Insurance – cybersecurity insurance (evolving market)

Data Security Incident? Now What…

- “Data Security Incident” ≠ “Data Breach”
- A Data Security Incident is a factual event
- A “Data Breach” is a ***Legal Conclusion***
- Follow Incident Investigation Process
- Escalate
- Execute Incident Response Plan (IRP)

Step 1: Contain

- Assess scope of incident.
- Take affected systems offline; OR
- Disconnect systems from network; OR
- Shut systems down altogether.
- Institute secure communications system.
- Convene Incident Response Team (IRT)
- Delegate tasks according to plan.

Step 2: Recover

- Spin up independent, clean systems
- Restore data from clean backups; OR
- Rebuild systems from clean images
- Inspect new systems for Indications of Compromise (IoC's)
- Validate
- Release to production

Step 3: Investigate

- Capture forensic investigation data:
  - Access, Firewall, security information and event management (SIEM) Logs
  - Device & Drive Images
  - Other Evidence of IoC
- Assess scope & extent of incident
- Make data breach determination

Step 4: Notice

- Determine nature of sensitive information
- Identify affected persons
- Identify notice obligations
- Draft notices
- Timely disseminate notices

Step 5: Remediate

- Address identified system vulnerabilities
- Counsel responsible persons
- Review & update technical compliance plans
- Review and update user security training

Incident Response Team

- General & Outside Counsel
- Agency Information System & Tech
- Forensic consultant
- Law enforcement
- Insurer
- Public Relations
- Breach Notification Services

Data Breach Response Issues

- Attorney-client privilege
- Forensics
- Law enforcement demand
- Public relations response
- Breach notification
- Credit monitoring
- Insurance claim and carrier resources

Internal Questions

- Do you have an internal privacy policy?
- Do you have a privacy policy posted on your website? When was it last updated?
- Who handles your data security? Is that person following a controls rubric?
- Have you tested your security systems?
- Do you know if you have coverage for a cyber incident and what costs are paid?
- Do you have a data incident response plan? Practiced it?