SheppardMullin

VIP Backstage Pass: Ethical Issues Responding to a Cyber Attack

January 29, 2020

Your VIP Backstage Tour Guides

Justine Phillips | Cyber Attorney
Sheppard, Mullin, Richter & Hampton LLP

Paul Najar | General Counsel
Gafcon, Inc.

What Is a “Data Breach” in California?

- Unencrypted personal information was acquired or reasonably believed to have been acquired by an unauthorized person.
  - (California Civil Code s. 1798.29(a) [agency] and California Civ. Code s. 1798.82(a) [person or business]).

- Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.
  - (California Civil Code s. 1798.29(e) [agency] and California Civ. Code s. 1798.82(f) [person or business]).

The Culprits

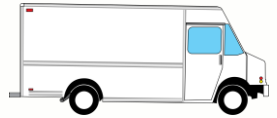
37%
Phishing

30%
Network Intrusion
(Hacking/Malware)

13%
Stolen/Lost Device
or Records

55%
Employee Action/
Mistake

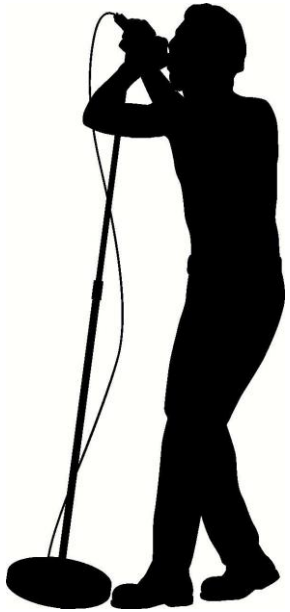
27%
Non-Vendor
Unrelated Third Party



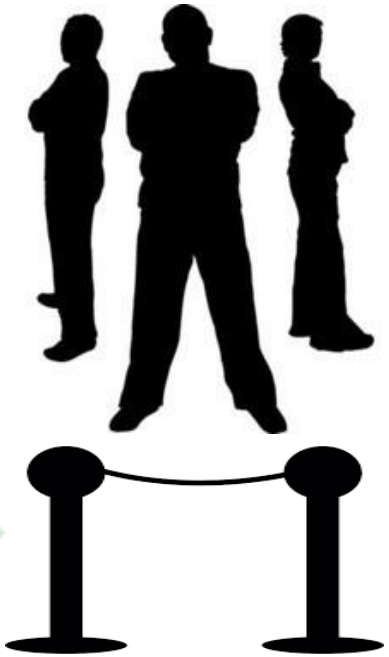
11%
Vendor

Source: Baker Hostetler's 2019 Data Security Incident Response Report

Cyber Threats: Any person, thing, or event that could violate system security policy



Industrial Control System Attack	Intended to disrupt or destroy activities of large-scale companies or organizations (often state-sponsored: e.g., Sony, Stuxnet, France TV5, US and Mexican election systems)
Organized Crime	Usually financially motivated, target corporate data such as personal information, health information, credit card numbers (e.g., Target)
Insiders	Employee or contractor using access to release or ex-filtrate information for personal, competitive, ideological or financial gain (e.g., WikiLeaks)
"Advanced Persistent Threat"	Organized, state-sponsored groups methodically infiltrating the enterprise, often maintain presence for months or years (e.g., Anthem, DNC)
"Hacktivism"	High-profile attacks for ideological motives, intended to embarrass, publicize, effect change (e.g., "Anonymous," Ashley Madison, "Panama Papers")
Ransomware	Systems and/or files encrypted and disabled; may be decrypted after payment of ransom
Espionage	Corporate- or state-sponsored theft of trade secrets, personal data



Ethics and Competence in Breach Investigations

Duty of Competence (CA Rule 1.1 – Formerly CA Rule 3-110)

- **CA Rule Change**: Diligence is now a separate rule (Rule 1.3)
- **Knowledge**: In-House Counsel ("IHC") must be aware of the following:
  - Benefits and risks associated with relevant technology
  - Legal obligations when a breach occurs.
  - How to respond competently (should at least have a cyber incident response plan)
- **Monitoring and Detection of Breaches**: IHC should make reasonable efforts to ensure the company monitors technology resources to detect a breach.

Ethics and Truthfulness in Statements to Others in Breach Investigations

Truthfulness in Statements to Others (CA Rule 4.1)

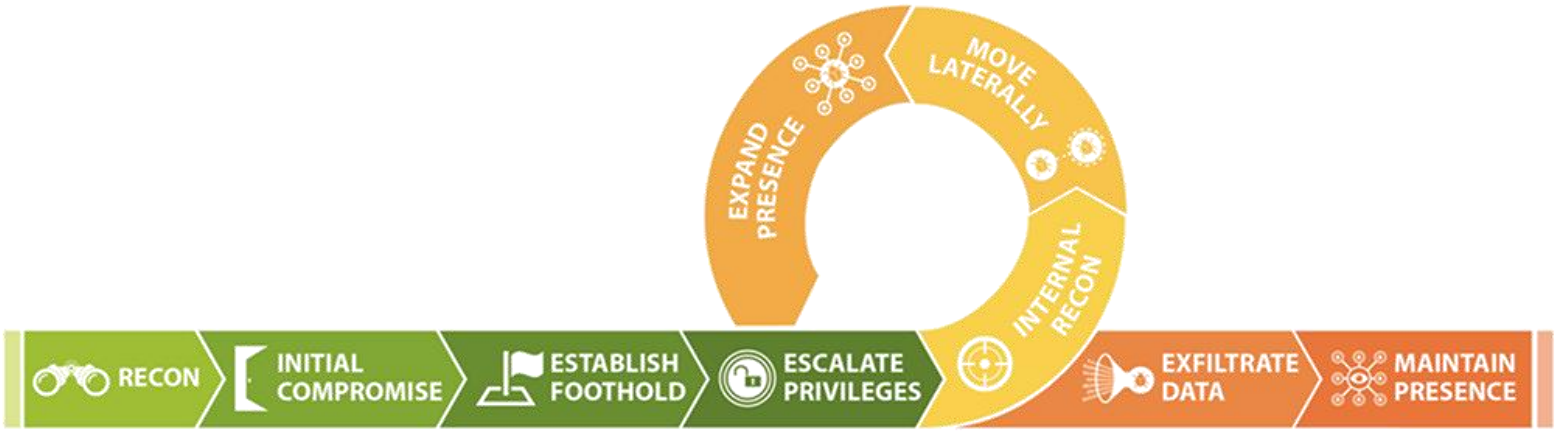
- **CA Rule Change**: This rule is new and has NO counterpart to the old California rules.
- **Rule: In representing a client, a lawyer shall not knowingly:**
  - make a false statement of material fact or law to a third person; or
  - fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client
- **Misrepresentations**: IHC often deal with third parties (both directly and indirectly) and must carefully avoid making or becoming entangled in misrepresentations.
  - A misrepresentation can occur if the lawyer incorporates or affirms a statement of another person that the lawyer knows is false.
  - Can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.

Ethics and Reporting Up in Breach Investigations

Organization as Client – Reporting Up: (CA Rule 1.13(b)-(e) – Formerly CA Rule 3-600(B)-(C))

- **Less Discretion**: Applies if lawyer "reasonably should know" of a violation of law.
  - Also applies for a violation of a legal obligation to the organization.
- **Narrower Scope of Applicability:** The violation must be reasonably imputable to the organization AND likely to result in substantial injury to the organization.
- **Reporting Up Obligation**: Where IHC knows the highest authority is in violation of the law, the duty to represent the organization does not end unless the IHC resigns/withdraws.
- **New Safe Harbor Provision**: A lawyer who is terminated for reporting up or forced to resign/withdraw "shall proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge, resignation, or withdrawal."

Anatomy of a Breach



- **Infiltration**
- **Exfiltration**
- **Access to Protected Data**

Triaging

- Forensic Investigation
- Law Enforcement
- PR Communications
- Corporate Governance
- Notification of Affected Individuals
- Threat Information Sharing with Government and/or Industry
- Consider Public Disclosure
- Insurance
- Contractual Obligations
- Regulatory Investigations
- Lawsuits
- Systems Remediation

Attorney-Client Privilege/Work Product Protection in Breach Investigations

Attorney-Client Privilege

- **Legal or Business Advice?**
  - Get outside counsel involved immediately.
  - Be careful of waiving privilege for disclosure.

OR

Work Product Protection

- **In Anticipation of Litigation?**
  - Internal audits or data security reports before breach or litigation may not be protected.
  - Have outside counsel retain and supervise third parties investigating breach.
  - Be strategic about the information contained in incident investigation reports.

Attorney-Client Privilege and Cyber Investigations

Tips for maintaining privilege:

1. Retain outside counsel.
2. Expressly state in retention agreements with technical experts that their services are being sought in anticipation of litigation.
3. Rigorously wall off your response teams.
4. Make sure your privilege team is actually rendering legal advice in anticipation of litigation.
5. Maintain a detailed privilege log.
6. Courts will deny application of the attorney-client privilege when the attorney merely acts as a conduit for analysis performed by the third-party investigator.
7. Create server images of affected servers

Cyber Incident Simulation

Haulin Oats, a California corporation, sells cereal products to customers in the United States and Canada.

- The company operates a standard e-commerce website, where customers can sign up to receive a monthly bucket of cereal.
- Customers must set up an account by entering their name, phone number, date of birth, address, credit card or PayPal.
- The company dominates the monthly cereal bucket market, largely from their most popular cereal, *Braneater*.
- Haulin Oats employs 1,000 people in locations around the United States.
- Haulin Oats is a little *out of touch* and uses Windows XP and backs up its data once every six months.

Incident Response Simulation: Mega Breach

Scenario:

- Over Super Bowl weekend, one of Haulin Oats' star employees, Beyoncé Knowles, was at the office attempting to finish a project. In the process of finalizing her project, Beyoncé received notification that a new file entitled "Destiny's File" had been placed in the DropBox folder created by one of the company's shipping vendors. Haulin Oats employees regularly used DropBox to easily share invoices, files, and contracts.
- Always an *independent woman*, Beyoncé decided to open DropBox and click on the link to download the recently added file. All of a sudden, a big red text box popped up on her screen. Panicked, Beyoncé immediately shut off her computer and attempted to restart her system. When the computer turned on, the same pop up appeared. Afraid of getting into trouble and ruining her reputation as a *survivor*, she just shut down her computer and went home.
- IT supervisor, Ron Jovi, receives notice that Beyoncé's computer is infected with a virus and the virus is laterally moving throughout company infecting other computers.
- By Monday, all computers, servers, phones, printers and systems are infected and fully encrypted by ransomware.

What next?

SheppardMullin

Debrief on Incident Response

- ❑ Do we have a “Top Down” Risk Management Approach from the C-Suite down to the Mail room, i.e., “from the board to the keyboard”?
- ❑ Strong Employee and IT Administrator Password Procedures?
- ❑ Clear Employee Procedures pertaining to Data Security and BYOD?
- ❑ Is the IT department integrated with Sales, Operations, Accounting, etc.?
- ❑ Do we know how many Personally Identifiable Records (PII) are in my company’s Care, Custody and Control?
- ❑ Do we Encrypt sensitive Personal Information? On Laptops and mobile devices as well?
- ❑ Do we have Virus Protection? Firewall Protection? If so, have my vendors been in the news lately about Security flaws in their offerings?
- ❑ Does my website have a Privacy Policy? Are we following it in every aspect of our business processes?
- ❑ Has your company established enterprise-wide guidelines for PII records and information management compliance?