When to Add Legal to Your California Data Breach Response Team: A "Just in Time" Model

Jill Bronfman
Director of Privacy and Technology Project
Adjunct Professor of Data Privacy Law
Institute for Innovation Law
University of California Hastings School of Law

Professional Strategies – S12

INTRODUCTION
CONTEXT/FOCUS AREA OF PRESENTATION
TAKEAWAYS…

Types of Data Breaches, Old and New

- Breaches can occur as the result of an **affirmative attack** during which an individual or group of individuals intentionally break into a network to capture data in transit, or into a database to capture data at rest, and view, destroy, or steal the data.
- Breaches can also occur due to **negligence or mistake**, such as when an employee of the company leaves a laptop in a taxi on the way to a meeting, or introduces a data mining virus into their home network from a USB drive they picked up on the way out of that meeting.
- Breaches that result from employee malfeasance or accidental leaks are called **insider threat**.

Shift in Data Protection

- Corporate proprietary information is information that belongs to a company and it is different from personal information that belongs to or identifies an individual. Companies are concerned about losing or leaking data that belongs to them, and also about losing the personal data with which they have been entrusted.
- Legally-protectable corporate proprietary data includes **trade secrets** like the formula for a soft drink, proprietary information such as **customer lists and sales data**, **intellectual property** still in development, **employment and employee data**, and **business processes** that are the essence of the corporation's success.

Shift in perceived responsibility for data breaches

- Data security expands beyond the IT department, to…
- C-suite responsibility
- Legal
- Public Relations
- Executives
- Security professionals
- Privacy professionals
- Marketing
- Government relations
- Customer care/HR
- Risk management and Insurance
- Law enforcement

Just in Time Legal Model

- Analogy from the manufacturing industry that wanted to avoid costly storage of products
- Eliminating waste by making only what is needed, when it is needed, and in the amount needed
- Factors in supply chain need to click together
- It's a communications effort!

How To

- Designated personnel should know what to do and when to do each activity
- Mix of Prepared Timelines & Checklists
- **Timelines** presuppose set patterns (based on prior experience)
- **Checklists** cover basics but allow for more flexibility when circumstances change

Extreme Scenarios

- **Very Early**: Legal is there on day zero, discovering the breach or being notified of the breach by outside sources, or, much later…
- **Very Late**: Legal is brought into the situation room after a complaint has been filed against the company

Ideal/Just in Time Legal Involvement

- When are you interviewing attorneys?
- *Note: They do not magically appear when you need them like guardian angels or godmothers in fairy tales. You have to interview and hire legal just like other corporate functions*
- When should you interview attorneys?
- Ex/ to help prepare or at least review your data breach plan
- Ex/ query existing GC or legal resources to survey their cybersecurity expertise

Dress Rehearsals

- Your table top **exercise** data breach should include at least one member of in house or outside counsel legal team
- That legal POC can then **waterfall** the lessons learned to other legal team members, saving legal costs
- Be sure to **survey** legal along with other team members to gather improvements and then **implement** them!

What Does Legal Need to Know? (and when do they need to know it?)

- Your in-house legal resources should be:
  - Educated in your business
  - Ready to respond to data breaches
  - Part of the breach response team
- Your outside legal resources should be:
  - Educated in your business
    - Prepared materials for outside distribution?
  - Ready to respond to data breaches
    - Get contact information for POC & have a backup plan
  - Part of the breach response team
    - But not part of business or technical discussion, because…

Preserve Attorney-Client Privilege

- Mark paper and electronic documents "Confidential" or "[Law Firm Name] Attorney-Client Privileged" or "[Company Name] Proprietary Information
- Nondisclosure Agreements to "flow down" your data breach requirements to vendors including attorneys and their vendors (cloud service providers)
- "Need to know basis" conversations

What should you do if you suspect a leak/breach of information?

- Pick up the phone, and call the POC attorney immediately.
- If you send an email, don't compound the problem by identifying (or attaching!) the information, but do mark the request as urgent.

California Rules

- On September 30, California attempted to step up to the plate and update its data breach privacy regulations with AB 1710. The amended portions of the law take effect January 1, 2015. The text of the bill is available at: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710

What do we have to do?

- The California amended law now requires:
- (1) for data breach notifications, if the person or business providing the notification was the source of the breach, that the person or business offer to provide appropriate **identity theft prevention and mitigation services**, *if any* [italics added], to the affected person at no cost for not less than 12 months if the breach exposed or may have exposed specified personal information, (2) that companies who **maintain data, in addition to those that own or license the data, now protect the data**, and (3) in addition to restrictions on disclosure of social security numbers, except as specified, **prohibit the sale, advertisement for sale, or offer to sell of an individual's social security number.**

Ramping Up to Meet Requirements

- Legal analysis of some of the ambiguous language in data breach notification bills
- Research a vendor for ID theft protection service. Consider whether your security incident meets the statutory thresholds for actual breach.
- Look at other states' laws as well, and pending federal legislation

Factors for Notification

- In each state notification statute, there are issues of legal interpretation…
  - What is the threshold for notice?
  - Who do you have to notify?
  - Are there any relevant exceptions to notice requirement?
  - What happens if you don't notify? (private right of action or state attorney general enforcement- latter is more common)

Data Minimization & Destruction Policies

- You can't lose data that you didn't collect
- You can't lose data that you didn't store or keep, so…
- Create a policy to reduce the amount of data you collect to the minimum needed to do business and destroy the rest according to industry standards (unless legal instructs you to keep certain data for regulatory or litigation hold reasons)
- Flow down the policies to vendors, including law firms

Resources

- HP videos at http://businessvalueexchange.com/blog/2015/07/01/lessons-to-be-learnt-from-ebola-not-something-you-often-hear/
- IAPP whitepaper, forms, & checklists at https://iapp.org/resources/issue/responding-to-a-breach/ (login required)
- Ping me at bronfmanj@uchastings.edu for updates, articles, and resources

Questions?