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

Jill Bronfman
Director of the Privacy and Technology Project
Institute for Innovation Law
University of California at Hastings College of the Law

Professional Strategies – S12

Session Abstract

Imagine you work for Anthem, Sony, Target, or whoever just hit the news, and you have been designated the point person to respond to the breach. Who is on your incident response team (Lawyers, IT, Executives, Security professionals, Privacy professionals, Marketing/PR, Government relations, Customer care/HR, Law enforcement and/or Risk management)? When should you bring legal into the equation and how can you efficiently and effectively use legal resources to solve common data breach dilemmas, such as law enforcement/media notification requirements and triggering insurance coverage? What information does a lawyer need to protect your company from liability, fines, or the glaring light of the media?

At this point, everyone should learn the basics of data breach response legal requirements. Recent headlines have highlighted research findings demonstrating that the public and the board of directors of your company now see the responsibility for data breaches and other security incidents as extended from data security professionals to the C-suite and beyond. For many executives as well as security professionals, it's now not enough to say I didn't know or it wasn't my job to protect the missing, damaged, or leaked data.

The types of companies affected by these law has expanded as well, for example, effective January 1, 2015, California law includes offering identity protection services for private citizens victimized by data breaches. The law expands the burden of protecting personal information beyond data owners to data storage companies. Companies who "maintain" this information may be responsible for identity protection services if a breach occurs, and for a host of other restrictions regarding selling SSNs and protecting personal information. Other states, and pending (possibly preemptive) federal legislation, may be poised to impose additional requirements for response to data breach as well.

It's time for a Just in Time Legal Model. "Just-in-time" manufacturing ideas center upon eliminating waste by making only what is needed, when it is needed, and in the amount needed. Additionally, much like the just-in-time manufacturing model depends on many factors in the supply chain to click together, the success of the incident response team depends on the competence and reliability of each of the individual team members (i.e., designated personnel should know what to do and when to do each activity). On the extreme edges of this model as applied to data breaches, either (a) legal is there on day zero (when the breach occurs), discovering the breach or being notified of the breach by outside sources, or, (b) legal is brought into the situation room after a complaint has been filed

against the company much later in the timeline. These dramatic set-ups are great pitches for reality television or blockbuster films, but in most situations, it's quite a bit more fluid as to when legal can or should become involved in the data breach response process. While the U.S. legal system emphasizes monetary solutions to remedy mistakes made, we can look at these mistakes and think about how to sidestep them in the future to save money, and we can try to avoid creating problems that are difficult to quantify and recompense, like the loss of privacy, identity, and trust.

This presentation will cover identifying incidents with legal import along the data breach timeline. We'll take a telephoto shot of data breach scenarios as they have played out in the news and in corporate boardrooms, and then focus in on the issue of legal involvement in the process. There are many unforeseeable weak spots in the continuity of data security, but having agile legal resources educated in your business and ready to respond with and to the team need not be one of them.

Target Audience

The audience for this session should be information security, assurance, risk management, and governance professionals who have some sophistication with the concepts of data security, but who wish to increase their understanding of when and how to interface with in-house and outside counsel in a rapid and effective manner and to preserve attorney-client privileges.

Speaker Bio

Jill Bronfman, Director of the Privacy and Technology Project at the Institute for Innovation Law and Adjunct Professor of Law in Data Privacy at UC Hastings College of the Law, was named to The Recorder's 2014 list of the 50 Women Leaders in Tech Law. Also, Professor Bronfman was selected as a 2014-2015 USC Annenberg Alumni Ambassador. Professor Bronfman was an Assistant General Counsel and Network Security and Privacy Subject Matter Expert for Verizon in the San Francisco office. At Verizon, she designed and moderated several in-house training programs in data security, compliance, and intellectual property. She also taught at San Francisco State University, including developing a new advanced seminar in Mobile Communications. At the National Association of Broadcasters/ Broadcast Educators' Association Conference (NAB/BEA) in Las Vegas, she presented "Mobile Communications 2014: What's After What's Next." In this presentation, she drew on her research in the field of privacy and technology to speak about the latest issues in drone regulation and the legal implications of 3D printing. Her article, "California Data Breach Law- Rounding the Bases," appeared in the ABA's Information Law Journal Spring 2015. Professor Bronfman has presented on privacy and security issues at the RSA and International Association of Privacy Professionals (IAPP) conferences in Spring 2015, and has had papers accepted for Berkeley Law Privacy Law Scholars Conference (PLSC) and Amsterdam Privacy Conference (APC2015). Professor Bronfman received a joint degree at USC in Law and Communications Management (JD/MA) and a dual undergraduate degree at UC Berkeley in Mass Communications and History.

Speaker Details (optional):

Twitter URL	@privacytechlaw
LinkedIn URL	https://www.linkedin.com/pub/jill-bronfman/5/4b7/63a
Website	http://innovation.uchastings.edu/focus-areas/privacy-and-technology/