1. Prepare Solid Foundation for Privilege
* Convene a data breach response team at request of inside/outside counsel
	+ Data breach response team provides information to inside/outside counsel to advise on legal ramifications of breach
	+ Document. Document. Document.
1. Verify the Data Breach
	* No notice given unless breach is confirmed
2. Identify and/or Convene A Data Breach Response Team
	* IT Personnel
	* Chief Privacy Officer
	* Security
	* HR
	* The leader of the business unit affected by the breach
	* A member of risk, internal audit or compliance team
	* PR/Communications team member
3. Conduct An Investigation
	* What type of breach occurred
	* How it occurred
	* The duration of the breach
	* What information was put at risk
	* The identity of the individuals affected by the breach
4. Assess Risk
	* Consider insurance
	* Review third party vendor contracts
	* What data breach notification laws apply to the information that has been compromised
	* Consider disciplinary action
	* Assess risks of litigation
5. Develop A Notification Plan
	* Distinguish between required and/or discretionary notice
	* Decide if a vendor is needed
	* Draft notice – consider all state content requirements
	* Make a list of the individuals and/or entities to whom notice must be sent
	* Maintain a list of the individuals notified – who, when and where
6. Develop A Communication Plan
	* Internal and external
	* Transparency and consistency is key
	* Identify point of contact for questions
7. Decide Whether Remediation Services Will Be Offered To Affected Individuals
	* California and Connecticut have requirements
	* Consider generating goodwill in the wake of a breach and in turn reducing potential damages
8. Taking A Step Back
	* Analyze the breach itself and the company’s response to the breach
	* How could it have been avoided
	* What proactive steps can be taken going forward
9. Have A Written Data Breach Response Plan
	* Serves as a guide for the team
	* Serves as Exhibit A for the company’s defense in the event litigation