Inside Counsel
SEPTEMBER 29, 2015
BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

An ALM Website
www.insidecounsel.com

BY REBECCA FELSENTHAL

Forget earthquakes: Building a data breach preparedness kit for your brand

Few phrases make brand owners more nervous than "information security" and "data breach."

FEW PHRASES MAKE BRAND owners more nervous than "information security" and "data breach." Today's in-house counsel must not only be a legal expert, but an expert in all aspects of her client's business, including technology.

Thus far, this six-article series has addressed five other niche areas of brand protection. The first article identified strategies for dealing with grey market goods. The second article discussed FCPA compliance. The third article outlined tips for fighting counterfeiting by collaborating with law enforcement. The fourth article was a primer on running a successful international counterfeit investigation, and the fifth article walked the reader through the keys to online monitoring. In this article, the final one in this series from Sideman & Bancroft attorneys, we will examine prophylactic data security measures for brand owners.

What is a data breach? Data breaches include the "hacks" of, or unauthorized access to, client and customer information. But a breach does not only happen in a digital space; a breach also occurs with the theft of a laptop or flash drive holding proprietary or trade secret information. Business entities of all sizes risk exposure for breaches. A small company that relies on a single IT employee for hardware and data security needs may lack the technological sophistication and the bandwidth to protect its data from loss. A large company, on the other hand, possesses a greater volume of data, operates more complex information systems, and faces more variables in constructing data security measures.

What are the consequences? A data breach does not just put personal and proprietary information at risk, it also exposes your organization to statutory liability. In nearly every state, the discovery of a data breach triggers some notification obligation; HIPAA, federal banking regulations, and the IRS have also imposed disclosure requirements. Whether notifying customers, agencies, or state attorney generals, notification obligations can become costly. There is no one-size-fits-all approach, as the regulations differ on the requirement of e-mail, mail, telephonic of substitute notice. A data breach also opens your organization up to regulatory enforcement actions, fines, and private causes of action. For example, the FTC brought an enforcement action against Fandango last year, alleging that it engaged in unfair and deceptive business practices by misrepresenting the security of its mobile app and failing to provide reasonable security in the transmission of customer data; the action was settled with an order requiring Fandango to undertake specified security measures. In 2012, Massachusetts

imposed $15,000 in fines and other compliance obligations on a Boston business when an unencrypted laptop containing the personal information of 621 consumers was stolen from an employee's car.

What can you do? The Federal Trade Commission (FTC) and the Department of Health and Human Services, among others, have adopted the "reasonable security" standard, a process-oriented standard that asks organizations to (i) assess risks, (ii) identify and implement security measures tailored to those risks, (iii) verify their effective implementation, and (iv) ensure that they are continually updated in response to changes in those risks. Adopting a handful of key prophylactic measures with an eye toward "reasonable security" can mean the difference between a data breach nightmare and a manageable, if unfortunate, threat to your organization's data security.

- **Conduct a risk assessment.** Working with outside consultants and legal experts, assess what data your organization has, and to whom that data belongs (*e.g.*, to the business, to a partner, to a customer). Identify what information systems hold that data, and where those systems are located. Evaluate the threats to your data – are they internal or external? What is the likelihood of the threat materializing, what damages will the threat make to my data security and to my brand, and what are the costs of repairing those damages? Repeat the risk assessment periodically as these circumstances will undoubtedly evolve.
- **Relevant security standards.** Determine what state and federal standards your data security needs to meet. dentify customer, partner, and vendor contracts that impose their own security obligations.
- **Policies.** Using your risk assessment, identify a baseline against which your policies and protocols can be evaluated. Remember to be reasonable; craft policies that balance the costs and burden of securing your data against the likelihood of the threat, the complexity of your organization, the nature of your business, and the capabilities of your infrastructure (and technology in general). Establishing strong policies isn't enough; train your team and ensure their compliance.
- **Critical instant response plan.** Design a plan that outlines protocols tailored to the level of the threat. A strong response team includes not only technology experts, but legal and public relations professionals as well. Allow outside counsel to investigate the breach to ensure that the results are objective, credible, and, if necessary, privileged. Prepare to make critical decisions within hours of discovering a data breach. An appropriate response plan does not aim to *stop* the breach; it aims to *handle* the breach by re-establishing the integrity and availability of your data system, identifying which data has been threatened, and determining the source of the threat.
- **Evaluating whether an actual breach occurred.** A threat to your data security does not always mean a breach has occurred. Many statutes and regulations possess an encryption safe harbor that insulates an organization from notification obligations if the threatened data is encrypted.
- **Defensive litigation.** Prepare for defensive litigation. Engaging in these prophylactic measures won't necessarily avoid litigation, but will prepare your organization to adequately defend against investigations, enforcement actions, and private lawsuits.

A data breach seems like a worst-case scenario, yet the question is not if, but when, a data breach will occur. Engaging in a few targeted and cost-effective steps can help your organization protect its data and its brand from major damage down the line. By building a careful and thoughtful data breach preparedness kit, your organization will be prepared to face threats to your data security, and minimize the impact of a breach to your operations and your brand.

CONTRIBUTING AUTHORS
REBECCA FELSENTHAL is an associate at Sideman & Bancroft in San Francisco. Working with the firm's Brand Integrity and Innovation Group, she represents business entities in connection with brand protection issues, trademark enforcement, and a range of civil litigation matters.