BROOKS PIERCE

How to Talk to Management about a Privacy

Digital Media and Data Privacy Law Blog

By Elizabeth Spainhour on 09.28.2015
Posted in Privacy

We've discussed the importance of privacy assessments here in the past. It is a frustrating realization, indeed, when a company discovers a data breach involving data that it never needed or even knew it kept.

A proactive company-wide privacy assessment allows your business to carefully evaluate on its own timeline (rather than in the panic of breach response) the company's data collection, sharing, storage, and security practices. Vulnerabilities can be identified and addressed, and "stale" privacy and security policies can be updated to reflect current practices.

Let's assume that you are on board with the importance of a privacy assessment. (You are, right?) How do you convince management that the benefits of taking time to conduct a privacy assessment outweigh the risks of diversion away from other priorities?

Here are a few reasons you can give your company's leaders to explain why they should authorize a privacy assessment:

1. **Regulators are serious about privacy, so you should be, too.** Federal and state regulators have made consumer privacy and data protection a top priority. The Federal Trade Commission, in particular, has been flexing its muscles in this area. Recently, in *FTC v. Wyndham Worldwide Corp.*, the Third Circuit upheld the FTC's "unfairness" authority to bring an administrative action against Wyndham for inadequate data security practices. The FTC has also exercised its "deception" authority to fine companies for (among other things) failing to live up to promises made in their written privacy and security policies. State Attorneys General are also key regulators in this area. For example, North Carolina's Attorney General includes identity theft among the top consumer protection issues of focus for his office. Enforcement actions are a real risk and simply cannot be ignored.
2. **Privacy matters for all businesses, not just the healthcare and financial services industries.** There's a temptation to think that if you're not in the healthcare or financial services fields, privacy isn't a significant risk. That is a faulty assumption. If your business collects information from customers or visitors to its website, or if your company holds sensitive information (employee social security numbers, for example), your company needs to confront and address data privacy and security policies and practices. Certain kinds of data are subject to regulation—do you know what, if any, regulated data your business has? An assessment will

help you answer this question.

3. **An assessment on the front end will save you time, energy, and money when it comes time to respond to a breach.** An ounce of prevention is worth a pound of cure. That's as true in the data privacy and security arena as any other. A privacy assessment that involves stakeholders from all areas of the business in the discussion—IT, marketing, human resources, legal—allows the company to understand and make informed choices about the data it collects, uses, and shares, and how it stores and disposes of that data. If your company has gone through a recent assessment, you will be ahead of the curve in the vital early hours and days of the discovery of a data breach.
4. **Insurance is important, but it is not a cure-all.** Insurance is a terrific and necessary arrow to have in your risk management quiver. But data privacy and security are complicated, and there is no single magic bullet. Insurance, fortunately, can address covered monetary losses. But insurance cannot address non-monetary harms like brand and reputation damage, which can result from a data breach. Yet a company's brand and reputation are key assets of the business. A privacy assessment that results in concrete action to address privacy risks is a step your company can take to protect its hard-won reputation and secure the brand.