An ounce of prevention is worth a pound of cure. Benjamin Franklin

As we begin the new year, it is a great time for businesses to perform audits on their insurance policies and privacy practices. An insurance policy audit conducted by experienced coverage counsel is a preventative tool Fortune 500 companies use to identify potential gaps in coverage along with potential coverage issues and exclusions in their policies that may lead to coverage litigation if not addressed. These audits educate companies on the strengths and weaknesses in their insurance portfolios and arm companies with the information needed to negotiate broader coverage and eliminate exclusions and gaps at renewal, potentially saving companies millions of dollars in uncovered claims or coverage litigation.

Similarly, privacy reviews allows a company (or other organization) to understand and assess the variety of consumer and personal data it collects, learn how it uses that data, and with whom is shares or discloses the data. Then--outside a crisis situation--the company can receive advice regarding the lawfulness of its privacy practices, areas of increased and perhaps unnecessary risks, and recommended remediation or implementation of best practices. One of the worst privacy problems a company can have is learning of a breach (say, computer intrusion) but not knowing what data is possesses and the different obligations that can flow from breaches of different kinds of data. With a completed privacy review in its rearview mirror, the company will be empowered to act quickly and make informed, intelligent decisions as privacy issues arise.

Below we discuss the steps counsel take when performing insurance policy audits and privacy reviews.

**Steps in an Insurance Policy Audit**

The goal of an insurance audit is to evaluate the current insurance program, determine whether the program meets a given company’s needs, and identify any potential gaps in coverage. Every year insurance policies and standard forms change, new exclusions are added to existing policies, and new insurance products are introduced into the market. Knowing what coverage your business has and what is available is critical. The following are the three steps that should be taken for a successful insurance audit.
Step One: Interview with in-house counsel, risk management team, and key executives

Before analyzing any policies, a meeting with in-house counsel, members of risk management, and key executives should be held to discuss historic and current liabilities and potential exposures, business needs and overall corporate strategy. At a minimum, the following items should be addressed:

- Any current or potential liability for ongoing and anticipated projects;
- Any anticipated corporate transactions and potential corporate and D&O liability exposures;
- An assessment of current privacy policies and an understanding of the collection, storage, and use of any confidential information;
- A review of all professional services offered by the company, subsidiaries, affiliates, and portfolio companies; and
- The extent to which the company provides additional insured status to other entities and the extent to which the company requires other entities to list the company as an additional insured and the scope of any such agreements.

Step Two: Analyze each insurance policy individually and then how it works with the other policies in the company’s insurance portfolio

The next step is to analyze each insurance policy. A counsel-conducted analysis significantly differs from and complements a broker’s policy analysis. For example, multiple issues, such as number of occurrences, trigger and allocation, batch clauses, and exhaustion language may significantly affect any ultimate insurance recovery and require a level of legal sophistication in an analysis of their potential impact. While no one can predict with any certainty insurance companies’ future interpretations of policy language, courts have addressed many phrases and words in certain jurisdictions and a legal policy audit will at least minimize some of the disputes coverage counsel see arise.

All lines of coverage should be reviewed, including but not limited to liability policies, first-party property policies, business interruption policies, directors and officers policies, errors and omissions policies, cyber risk policies, employment practices policies, transportation and auto policies, fiduciary policies, fidelity and crime policies, and any specialty policies (e.g., products, IP, pollution). The review should include an analysis of the following provisions through a legal lens:

- coverage provisions, including definitions, extensions, exclusions, endorsements, notice and discovery provisions, defense costs, duty to cooperate, and right to settle claims and state variations;
choice of law and dispute resolution provisions;

deductibles, self insured retentions and retrospective premium provisions in light of the company’s business needs, overall objectives, and strategy;

trigger and discovery provisions and the company’s policies for providing notice to insurers;

underwriting requirements and disclosures provided to insurers regarding anticipated acquisitions and other corporate transactions;

analysis of how the primary, umbrella, and excess policies fit together in a single line of coverage; and

analysis of how the insurance portfolio interacts together as a whole.

Each company and industry will have different areas within their insurance policies that will impact insurance recovery. Identification of these specific issues will assist the company in describing any future claim in ways that will maximize its protection under the insurance program.

**Step Three: Compile a list of gaps in coverage and policy revisions to discuss with your broker**

The last step in an audit is the compilation of a list of all identified gaps in coverage and policy revisions that should be requested at the next renewal or earlier if significant gaps were identified. Often, companies request coverage counsel to prepare a memorandum that can be shared with the board and that contains this information along with examples of how the policy works and, when applicable, doesn’t work so the board can assess and understand the current coverage protecting the company and assess the need for any additional coverage. Since the attorney-client privilege may not extend to your company's broker, we do not recommend sharing the legal coverage audit with your broker. Instead we recommend creating a checklist of items requested to be revised for your broker that is devoid of any reasoning or comments.

**Steps in a Privacy Review**

Today, Rule No. 1 in complying with privacy laws and obligations is *knowing your data*. That bears repeating, even if it was just in italics: companies must know what data they collect, how they use that data, and with whom they share or disclose it, in order to know that those practices are lawful and do not carry with them undue risk. Moreover, when a potential privacy violation exists, such as a suspected network intrusion, almost all decisions will flow from knowing what data may have been affected or compromised. And a time of crisis is not the time to first have to assess what data the company holds.
Before going through the steps in a privacy review, there are two important concepts to go over: what is the data that we’re concerned about, and what are the practices to scrutinize? In the business world, privacy involves data belonging to or relating to consumers, members of the public, and others who are not a part of the company and therefore subject to its employee policies. This kind of data can be referred to as personal information or personally identifiable information (“PII”).

The practices that are regulated and scrutinized can always be broken down in the same way, regardless of the company or organization:

- collection;
- use; and
- disclosure.

Those are the three things that companies do with PII, and the many privacy-related requirements found in federal and state law also are organized generally around collection, use and disclosure of data and prohibit or otherwise regulate activities that fall under one or more of those three categories.

**Step One: Prepare for Interviews and Limited Document Collection (Mostly Policies)**

Start with an organization chart and identify every component that either serves a unique function or runs a separate operation. For example, sales, marketing, finance, security and procurement operations will each have different data needs and practices. Determine who a knowledgeable person from each such component is and schedule time to meet. After an interview list is created, consider all of the ways in which the company may collect data from or about others and consider whether the people on the list can speak to all of those collections, or if other sources are required.

**Step Two: Interview Manager in Each Company Area; Collect Policies and Data Maps as You Proceed**

There are different models for privacy reviews but the one we favor is following the data through the company. If you can determine all of the kinds of data that are collected, then you can simply follow each kind of data through the company (“And what is done with that information after it is collected?”) to see how it is stored, safeguarded and used. The final step, after finding all of the data that is collected and determining how it is used, is understanding what data leaves the company, and under that conditions that happens (e.g., Is data anonymized before sharing? Is it shared pursuant to contract?).

Along the way, interviewees will know of specific written policies that govern privacy practices—both public-facing policies and internal policies. Likewise, “data maps” may exist, which list or
categorize types of data or show where data resides and how it transits the company network. These polices and maps are important for understanding the company’s practices and for applying relevant laws.

**Step Three: Apply U.S. Law (and Foreign Law if Applicable) to Determine Need for Remediation and Updating Practices**

Privacy laws and regulations address collection, use and disclosure of data under a variety of legal schemes. Consumer protection laws and the FTC focus on unfair and deceptive trade practices, so clear notice must be given before data is collected. There are payment-card industry rules for storage of credit card information and Sarbanes-Oxley obligations with regard to adequate internal controls. And the alphabet soup of regulations governing disclosures of information include the ECPA, FDCPA and CAN-SPAM. Counsel will look at the company’s collection, use and disclosure practices and report on unlawful practices, high risk practices and opportunities to employ best practices.

An ounce of prevention may well have been worth a pound of cure in Benjamin Franklin’s day. But today, when that ounce of prevention is applied to insurance policies and privacy practices, it’s worth a whole lot more, namely, resting better at night knowing that your insurance coverage is what you expect it to be, and your privacy practices are not about to embarrass you when you least expect it.

Michael Sussmann, a Partner in Perkins Coie’s Privacy and Security practice, can be reached at MSussmann@perkinscoie.com and (202) 654-6333.

Selena J. Linde, a Partner in Perkins Coie’s Insurance Coverage practice, can be reached at SLinde@perkinscoie.com and (202) 654-6221.