If you face privacy issues on a regular basis, then you probably need a CPO.

**RECENT STATUTORY** and regulatory developments in the United States and overseas (especially Europe) have created near-paranoia about privacy in certain corporate circles. Headline-grabbing stories of actions by the Federal Trade Commission, state regulators, and consumer advocates have also demonstrated that a company’s customer and employee relationships, and perhaps its economic health, may depend in large measure upon whether the company is following “best practices” regarding data privacy and security.

Part of the response, for many large corporations, has been the creation of a new position within the corporate structure: that of the Chief Privacy Officer (“CPO”). Major companies, like American Express, AT&T, IBM, and many others in the Fortune 500, have announced within the past few years the development of a CPO position. There is little question that establishment of a CPO function within a corporation is desirable; but is it necessary in every instance? What of small, or medium-sized businesses, which may not be able to afford to hire a full-time CPO? This article briefly explores whether you really need a CPO.
DEFINING THE CPO ROLE • Before you can determine whether you need a CPO, it is worthwhile to review the role of the CPO in the modern American business. The function can vary greatly between corporations, but in broad terms, the role of the CPO is to help:

• Create and revise policies regarding privacy and security for confidential information;
• Train employees and staff regarding the company’s privacy policies;
• Ensure enforcement of the policies;
• Audit and document compliance with the policies; and
• Respond to new legislative and regulatory directives.

What becomes immediately apparent, on review of these elements of the CPO role, is that a CPO must have several different skills. A CPO must have some knowledge of relevant privacy and data security laws (many CPOs are lawyers). A CPO must also have technical knowledge, and the ability to identify how a company manages information, through the cycle of intake/creation, use and distribution, and storage and disposal. And a CPO must have management skills, as the process of creating, implementing, and revising privacy policies is essentially one long (actually, never-ending) corporate project.

Even a brief review of the elements of the CPO role confirms that CPOs cannot possibly perform their tasks alone. They must draw on knowledge, skills, and experience scattered throughout the corporation: general counsel, information technology, human resources, risk control, marketing, and many other departments often must be involved. Creation of viable privacy and security policies, moreover, requires a CPO to listen carefully to the needs expressed by various components of the corporation. A privacy policy created by fiat, which is not responsive to the corporation’s actual practices and business needs, may be bound to fail. And a privacy policy that is not understood, or a policy that is not viewed as beneficial to the corporate mission, may not be effectively implemented.

ALTERNATIVES • In many corporate organizations, CPO tasks require the full-time attention of at least one person. There are alternatives, however. Among them:

• Privacy Committee. A corporation might create a committee, consisting of representatives from the departments that have particular interest in privacy and data security matters, and those that should have input into any privacy policies. The challenge for such a committee is to ensure that the many, sometimes disparate, voices within a corporation are heard, and harmonized. Senior leadership within the company ultimately must take charge of finalizing and implementing the recommendations of the committee to avoid the “analysis paralysis” that can sometimes develop in group settings. It may be desirable to appoint a chair of the committee, who will serve, in practical terms, as a part-time CPO;
• Outside consultants. Law firms, accounting firms and (increasingly) data privacy and security consultants have much to offer corporations. Such consultants can suggest model policies, and can conduct helpful training and orientation for corporate managers and employees. Such consultants, moreover, may be engaged to conduct periodic audits of a company’s privacy practices, and report recommendations for improvement (perhaps to the corporation’s privacy committee);
• Professional organizations. In the past few years, several organizations have been created that are dedicated to the study and development of “best practices” with regard to privacy
and data security. Among these is Privacy & American Business, which conducts frequent workshops and seminars on privacy issues. The Better Business Bureau (“BBB”), moreover, recently announced development of a national initiative to help small businesses protect customer and employee data. The BBB has developed a “toolkit” to inform smaller businesses about the essentials of good privacy practices, outlining essential steps in a variety of areas.

The approaches listed above are not mutually exclusive. A business might well combine several of these (and other) approaches. For example, at the outset of a privacy initiative, a corporation might gather information from professional organizations, and invite consultants to provide training and insight to aid the formation of a privacy committee. Once the committee is operating effectively, however, the consultants might serve in a more limited capacity, providing updates on new privacy and data security regulations, and offering tips on new technology and practices. The assessment of the committee and consultants may, moreover, eventually warrant the hiring of a CPO for the company. The choice of a CPO, at that point, should be much better informed and attuned to the particular needs of the corporation as a result of the groundwork the committee and consultants have already done.

ADVANTAGES • Even if a company cannot employ a full-time CPO, the approaches outlined above offer several advantages:
• Establish “best practices” early. Small businesses, and those expanding into new areas, have unique opportunities to establish privacy and data security best practices from the outset of operations. Integrating such practices into the business early on may be cheaper, and much more effective, than attempting to impose such practices after technological and managerial structures have become entrenched;
• Plan for change. Businesses expand; new operations commence; technology changes. A company with a framework for dealing with privacy issues can more efficiently adapt to growth and change. Indeed, the development of such a framework should help the corporation embrace change, as an opportunity to implement new best practices, when they become available;
• Prepare for crisis. Headline-grabbing stories of investigations, lawsuits, and consumer (and employee) complaints about privacy and data security breaches can adversely affect even the mightiest corporations. So much more are smaller businesses at risk. The establishment of good privacy and data security practices, backed by a commitment of resources, and assignment of responsibility for implementing such practices, may be some of the best insurance the company can buy. Such practices and structures may prevent some of the worst crises that have affected American businesses. And, if a crisis hits, a company with defensible policies and a clear commitment to best practices can claim the moral and legal high ground, in ways that may defuse or at least minimize the crisis.

CONCLUSION • Data privacy and security laws are complex and ever-changing. And in one form or another, they affect virtually all American businesses. Whether a company should hire a full-time CPO is an inquiry that requires a careful assessment of the cost involved and the likely risks and benefits. Establishing a CPO position can be expensive; but there is no question that the liabilities for privacy violations can be staggering, not only in financial terms—but in terms of a company’s reputation.
Privacy and security matters are becoming ever-more urgent to businesses. Depending on the kinds of information that a business uses, it can be a very good idea to have a Chief Privacy Officer ("CPO").

- A CPO can:
  - Create and revise policies regarding privacy and security for confidential information;
  - Train employees and staff regarding the privacy policies;
  - Ensure enforcement of the policies;
  - Audit and document compliance with the policies; and
  - Respond to new legislative and regulatory directives.

- If a company cannot afford to create a CPO position, there are alternatives, including:
  - The creation of a privacy committee, with representatives from the departments that have particular interest in privacy and data security matters, and those that should have input into any privacy policies;
  - Outside consultants that can suggest model policies, conduct training and orientation, supervise or conduct periodic audits of a company’s privacy practices, and recommend improvements;
  - Professional organizations are dedicated to the study and development of “best practices” with regard to privacy and data security, such as Privacy & American Business and The Better Business Bureau.