Perspective//

//// State of the Chief Privacy Officer: Financial Services

by Brooke Sweeney

October 8, 2019

The United States is known for having the toughest regulatory standards for Financial Institutions (FIs) globally, yet is lagging behind when it comes to privacy. However, in the midst of a quickly evolving regulatory landscape, the need to develop a well-structured privacy function is crucial.

Over the course of the past several years, privacy has evolved from a best practice to one that has become mandatory and essential for companies who collect personal information from consumers. The European Union has led the way with the implementation of the General Data Protection Regulation (**GDPR**), which went into effect on May 25, 2018, and served as a global signal of the EU's dedication to privacy. Only recently, the United States has begun to follow suit with the California Consumer Privacy Act (**CCPA**), slated to go into effect on January 1, 2020. These monumental laws have resulted in increased awareness of privacy from not only companies, but also consumers who are becoming more informed about their personal data and how it's being used.

As a result, the role of the Chief Privacy Officer (CPO) has become a critical function in order to comply with increasing regulatory pressures. In order to keep up with rapidly changing and developing laws, **partnerships with other functions** have shifted. Historically, Chief Privacy Officers primarily worked with the Chief Information Security Officer (CISO), a relationship required for proper incident response to data breaches. While the CPO/CISO partnership is still vital, Chief Privacy Officers have also begun to interact closely with the Chief Data Officer (CDO). This is essential for successful **privacy by design**. In the shift to interacting with not just the CISO on a regular basis, but also the CDO, privacy initiatives have largely transitioned from reactive to proactive.

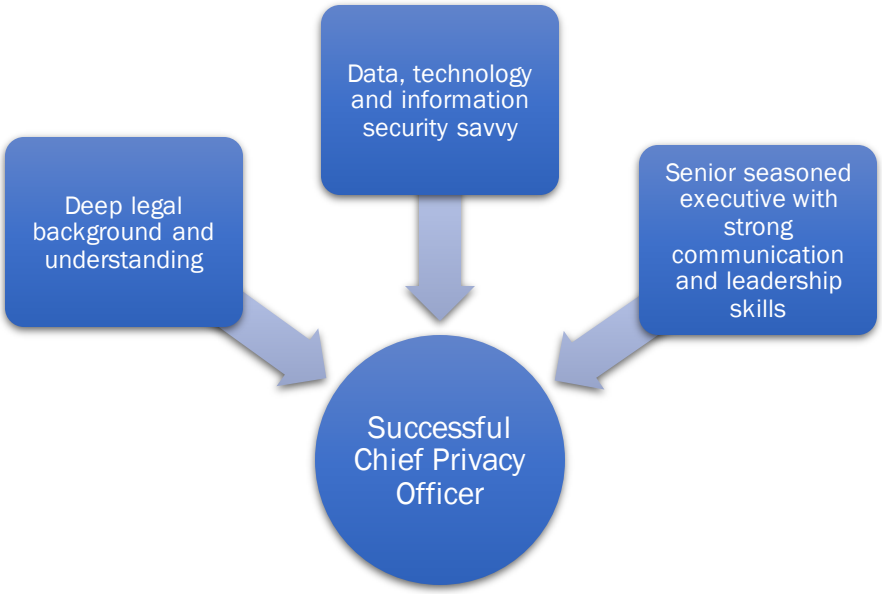
In many FIs, the **reporting line** of the Chief Privacy Officer role has also shifted. In the past, CPOs were typically positioned within legal, for example aligned to a direct report of the General Counsel. While this is still the case for some banks, it is increasingly common for the reporting lines of CPOs to now report up through enterprise risk management or compliance, for example reporting up to the Chief Compliance Officer. While not all banks have made this shift, this trend is a clear signal that privacy is becoming a priority for compliance and risk.

Other notable responsibilities and challenges for Chief Privacy Officers which have emerged:

1. Building a flexible program which can adjust for conflicting compliance regulations such as the GDPR and CCPA. This is especially challenging given that the laws are years behind technology.
2. Building a strong privacy team in a market with a high demand for talent, especially individuals with program development and implementation experience.
3. The increasing nature of threats to privacy, such as attempts to steal information and data breaches, have created a significant reputational risk for Financial Institutions.
4. The absolute need for a thorough understanding of company data, and a strong handle of the scope of that information.

SECONDLINE// ADVISORS//

The Chief Privacy Officer is a fast paced, highly integrated role that faces complex demands as a result of today's evolving landscape. Senior seasoned executives who have a thorough understanding of **both information security and the legal environment**, including the changing rules and regulations, are best positioned to be successful. Further, CPOs must be able to manage a cross functional team and maintain constant contact and communication with all other segments of the organization. Recently, more attorneys are stepping into the role and broadening their legal skillsets to more technology, data and vendor risk management.



Of the **current Chief Privacy Officers at the top 20 U.S. banks**, nearly 50% hold a law degree (JD). In addition, it is just as common for the role to have been filled internally versus externally, and gender diversity is almost equal. Further, the average tenure is about 5 years.

For what was once a part time job that was largely overlooked and considered a 'check-the-box' item, privacy is quickly increasing in prominence across the board. New and expanding regulations will inevitably force regulators to turn their attention to privacy, and in turn, further elevate the role of the Chief Privacy Officer. In addition, the **demand for privacy talent is increasing**, as companies are actively building out their privacy functions. Going forward, it will be crucial to be equipped with the right talent on all levels in order build, maintain and support a successful privacy program.

About the Author:

Brooke Sweeney joined Second Line Advisors as an Associate in July of 2019. She is establishing the firm's Privacy and Data Protection practice specifically within Financial Services. Prior to entering the executive search industry, she interned at Ad Age, where she worked closely with the marketing, sales and events teams. She holds a Bachelor of Arts degree from Colgate University, where she majored in Psychology and minored in Political Science.

Brooke can be contacted at: (646) 798-0814 or bsweeney@secondlineadvisors.com