CPO and CISO: The Evolving Roles of Privacy and Security Professionals

Technology, Privacy, and eCommerce

This article is the first in a two-part series, inspired by a presentation featuring Debra Bromson, Deena Coffman, and Ashley Slavik along with the authors.

Two major roles within companies are increasingly coming under review for applicability within varying data protection requirements. The Chief Privacy Officer (CPO) and the Chief Information

Security Officer (CISO) — or an employee with similar responsibilities — are responsible for what may be viewed as mutually exclusive responsibilities, but no longer. Their roles and responsibilities seem both to overlap and clash. Please note that “chief” does not necessarily denote C-level status. When it comes to compliance roles in general, “chief” often means the top person in the role, not a c-level designation.

With changes in the current regulatory environment, consider the European Union’s upcoming General Data Protection Regulation (GDPR), the New York Department of Financial Services, and China’s recently enacted Cyber Law. The roles of the CPO and CISO are becoming more recognized, more required, and more collaborative — not as siloed roles within in an organization but as partners.

Overview of the roles

The role of the CISO and the CPO differ in reporting structure, scope, and authority.

The CPO is responsible for the vision, strategy, and program regarding use of personal information. The CISO is responsible for the vision, strategy, and program to ensure protection of information assets, and technologies. From a reporting standpoint, the CPO often reports to either a general counsel, chief compliance officer and may have a dotted line to a board of directors. In contrast, the CISO may report to either the chief technology officer, chief information officer (CIO), or perhaps, a CEO directly and may also have a dotted line to the board.

In many cases, the CPO may have grown into the role from within the organization coming from IT, compliance, or HR. Prior to its recent prominence, privacy was considered a mundane part-time function tacked onto existing responsibilities. Organizations would ask for people to volunteer to take on this role to fill a gap. Over time, the privacy officer has gained expertise by necessity or is a lawyer who may have morphed into the role. The CISO, however, usually comes from within an IT function (network infrastructure, software development etc.) or may have been a former engineer who has continued to stay abreast of changing technologies.

However, as it relates to policies, vendor management, data breaches, and reporting to the board of directors, both the CISO and CPO play an integral and sometimes overlapping role to protect the brand and reputation of an organization. Their roles as collaborators and partners have become increasingly important.

In this series, we view the roles as separate positions, but there is a movement where the roles are combined. When combined, the one-role generally meshes into one of two formulas: The CPO takes both and has a strong information security person to rely upon, not as a direct report, but as a partner. The privacy and security officer may manage the policies, while the infosec manages the technical implementation. In the other direction — where the CISO takes on privacy — there tends to be a less well-defined scope of expertise. The chief data protection officer (or some similar title) may or may not have a separate privacy office to rely upon and may choose, instead, to send technical personnel for privacy training. Neither option seems to be ideal across the board; an entity would need to decide what works best for its regulatory situation, priorities, and culture.

In essence, no security is infallible and no privacy is absolute. An entity needs both to be successful.

Policy ownership

The CPO is typically responsible for the following policies, or if not, should contribute significantly to the final policy:

- Website privacy policy;
- Internal privacy policies (e.g., employee privacy policy, code of conduct privacy shield policy — if applicable);
- Data classification standards;
- Data subject access request standards; and,
- Social media policy.

The CISO should be responsible for the following:

- Security standards and requirements;
- Acceptable use policy;
- Data loss prevention software;
- Device inventory;
- Removable media control; and,
- Access control, provisioning, logs.

However, within each of the policies above, the roles should collaborate and likely involve other departments as applicable. There are quite a few policies where the two offices need to collaborate to have a comprehensive set of policies and approaches. These include:

- Vendor management guidelines, vendor standards, and due diligence;
- Acceptable use policy (also BYOD, Monitoring, etc.);
- Data breach, incident response policy, and procedures;
- Employee training and,
- Data classification and management.

And there are policies neither seems to want to own, but both CPO and CISO have a responsibility towards these policies (e.g., data retention policies and employee off-boarding).

Vendor management

With many regulations requiring due diligence, oversight, and control over vendors (consider, the GDPR), vendor management is a key risk and vulnerability for organizations. Since there is a general lack of confidence in the vendor relationship, ask the following questions before working with the vendor:

- Has the vendor disclosed or can you confirm if a vendor has had a data breach or cyber attack involving sensitive confidential information?
- Can you determine the number of vendors with access to their confidential information and how many of these vendors are sharing this data with one or more of their vendors?
- Do these vendors have data safeguards, security policies, and procedures that are equivalent to what you currently have in place?
- Is their security posture sufficient to respond to a data breach or cyber attack?

Despite this lack of confidence and in spite of the requirements to exercise control, companies rarely conduct initial or ongoing vendor reviews of vendor management policies and programs to ensure they address vendor risk. A lack of resources makes it difficult for organizations to have a robust

vendor management program. Companies rely on contractual obligations instead of audits and assessments to evaluate the security and privacy practices of vendors.

The requirement for oversight tends to land on the CPO and CISO, because executives and boards of directors are rarely involved in vendor risk management. It is worth noting, however, in the event of an incident, such as a major data breach or security breach, it is the CISO and perhaps the CEO who are held directly responsible — even if the vendor is at fault.

To address vendor oversight, the CPO and CISO should work together to perform due diligence and exercise ongoing oversight in combination with legal and the business unit who benefits from the services and products. Available tools include initial due diligence, independent vendor audit reports, such as a service organization controls report, type 2 for privacy controls (SOC2), and developing standards around the five trust service principles:

- **Security:** The system is protected against unauthorized access, use, or modification.
- **Availability:** The system is available for operation and use as committed or agreed.
- **Processing integrity:** System processing is complete, valid, accurate, timely, and authorized.
- **Confidentiality:** Information designated as confidential is protected as committed or agreed.
- **Privacy:** The system's collection, use, retention, disclosure, and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CICA.

Entities tend to want to keep their policies sacred, but the customer has a legal requirement to exercise due diligence. Whether you are the CPO/CISO on the customer side or the vendor side, you must be prepared to share policies to fulfill oversight requirements. These include all the policies listed above, along with proof of following the policies. In addition, CISO needs to establish a risk-based approach to test security measures of the vendors — and be prepared for customers to test your own.

Be sure to read the second part of this series, as we explore how CPOs and CISOs prepare for data breaches, draft contracts, and their roles with the board of directors.

Maggie Gloeckle

VP of Privacy and Compliance Counsel

A+E Networks

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.