Aug 10th, 12:00 AM

Exploring the Characteristics and Needs of the Chief Privacy Officer in Organizations

John G. Fehr III
Dakota State University, john.fehr@trojans.dsu.edu

Aaron M. French
Kennesaw State University, afrenc20@kennesaw.edu

Exploring the Characteristics and Needs of the Chief Privacy Officer in Organizations

Emergent Research Forum (ERF)

John G. Fehr III
Dakota State University
John.Fehr@trojans.dsu.edu

Aaron M. French
Kennesaw State University
afrenc20@kennesaw.edu

Abstract

Over the past two decades, the growth in technology (i.e. social networking, big data, smartphones, Internet of Things, artificial intelligence, etc.) and increased collection of customer data mixed with various data breaches has increased the need to focus more on information privacy. Various laws and regulations have been established, such as the GDPR in Europe and various state level regulations in the United States, to ensure the protection of customers and their data. The Chief Privacy Officer role was established in the 1990's with a strong research focus in the early 2000s. However, little attention has been given to the role of the CPO in the past decade. Due to the increases in technology, private data collections, breaches, and privacy regulations, there is a need to reevaluate the role of the CPO and the evolving responsibilities it entails.

Keywords

Chief Privacy Officer, Data Privacy Officer, DPO, CPO, Data Privacy, Data Privacy oversight, Data Privacy program

Introduction

Jennifer Barrett Glasgow became the first Chief Privacy Officer (CPO) in the United States in 1991 (ACDS, 2020), a role that would become formally established in 1999 due to the growing use of Internet technology (Brown, 2014). Today, data privacy oversight and regulation compliance is more important than ever due to technology growth (i.e., social networking, smart technology, IoT, Big Data, etc.) and new regulations and privacy laws. Consumer trust and brand reputation has degraded in recent years due to mishandling of data, unethical use of data, and data breaches (Salvi, 2021). Companies need to increase their responsibility and oversight of how they collect and handle private data and this elevated oversight and responsibility falls on the shoulder of a CPO (Hadley, Jr., 2018). Companies have privacy experts working in departments like engineering and legal, they often do not have a person in a leadership role to coordinate, manage, and oversee their privacy program and the policies associated with privacy (Edelstein, 2018).

In the early 2000's, various research evaluated the emerging role of the CPO in relation to growing privacy concerns due to online profiling (Marshall, 2001), CPO responsibilities (Pemberton, 2002), job functions and competencies of a CPO (Kayworth et al, 2005), and recommendations for expanding the responsibilities of the CPO (Sipior and Ward, 2001). Some regulations require a privacy officer be in place such as the General Data Protection Regulation, which specifically requires a data protection officer (Ashbel, 2020). Organizations trying to comply with those regulations have or wish to have a CPO often do not know what characteristics are needed to have a person in a leadership role guiding their data privacy program. (Privacy Commissioner, 2020). Based on this, the current study evaluates the following research questions.

- R1: What are the characteristics of a CPO?
- R2: How do we assess the need for a CPO?

While the role of the CPO received significant attention in the early 2000's, research on this role has been stagnant for more than a decade. The current research refreshes the view of the CPO to evaluate how this position has evolved over the past two decades with the growth of technology (i.e. smartphones, social

networking, big data, artificial intelligence, etc.), collection of personally identifiable information, and privacy laws. This research will examine the complexity of roles and responsibilities required by the CPO and qualifications required for this position. Finally, a model will be established to help organizations identify the need for a CPO based on the organization's informational needs, size of the company, information requirements, and other factors identified through our analysis.

To complete this research, we will first conduct a background analysis on the evolving role of the CPO and growth in data privacy including laws and regulations. Next, we will conduct a qualitative analysis interviewing CPOs to understand their roles and responsibilities along with interviews with organizations that do not have a CPO to evaluate how they address privacy and compliance issues. Next, we will conduct an analysis to evaluate current views of the CPO role and establish criteria for evaluating the need for a CPO role within the organization. We will conclude with a discussion of our findings citing theoretical and practical contributions with recommendations for future research.

Background

There are various roles in the industry that deal with privacy and security such as the Chief Information Security Officer (CISO), Chief Security Officer (CSO), Data Protection Officer (DPO), and the Chief Privacy Officer (CPO). Each of these roles handle various aspects of privacy and security. While CSO and CISO are sometimes used interchangeably (Glen, 2020), they are definitionally different with the CSO focused on the entire security needs of a company and the CISO being responsible for structuring security needs with the business objectives (von Ogden, 2014). While the CSO and CISO are more security related, the DPO and CPO bear the responsibilities of privacy assurance and compliance. In Europe, the General Data Protection Regulation requires organizations to have a formal role for a DPO (EDPS, 2022). Both the DPO and CPO are responsible for regulation compliance within the organization, the DPO does not have power to independently make decisions as CPOs often do (Coos, 2020). Figure 1 outlines a comparison of these four roles based on the cross section of privacy and security with responsibilities related to planning and execution.

	Security	**Privacy**
Planning	Chief Security Officer (CSO)	Chief Privacy Officer (CPO)
Execution	Chief Information Security Officer (CISO)	Data Protection Officer (DPO)

Figure 1: Differentiating Privacy and Security Roles

While privacy and security go hand in hand, the roles that address each are different and come with specialized knowledge and skills. The CSO and CISO have domain knowledge in cybersecurity and are often more technical in nature whereas the CPO and DPO have domain knowledge more embedded in laws and regulations. Many organizations often use synonymous descriptions for the CSO and CISO roles as well as the CPO and DPO roles, however, the key difference between them is planning and execution. The CISO and DPO typically execute the plans to achieve the objectives of security and privacy. These roles often report to other executive level position. The CSO and CPO is where privacy and security reach the executive level as these roles are conduct the strategic planning to address privacy and security. These roles are concerned with the welfare of the organization and have decision making power. The CPO may appoint two or more DPOs as needed based organizational needs (Clark, 2020). While the CPO is responsible for regulatory compliance, the daily monitoring of regulations and legislation as laws change and new policies are put in place falls on the DPO.

Many laws have been expanded and new regulations established in the past several years. Due to increased attention to data privacy and new regulations, the role of the CPO has evolved and needs to be redefined. The next two sections will dive deeper into data privacy and regulations that generate the need for a CPO and the standard view of the CPO role.

Data Privacy and Regulations

Data privacy is the right of individuals to control how their information is collected, shared, and stored (IAPP, 2022). Private information can be personally identifiable information of the individual such as name, location, contact information, or personally meaningful data such as online or real-world behavior and interactions (Cloudflare, 2022). Private information is being collected and shared, many times unknowingly, by organizations that use third parties, cloud service providers, and providers to the cloud service providers. Organizations, both domestic and international, are continually collecting more private data in an interconnected fashion integrating organizational data with various third-party data. Customers may be unaware if their data is being used or how. Private data collected within organizations needs to be tracked from end-to-end with the approval of those it belongs to.

Due to the sensitive nature and hardship to individuals that could ensue due to its misuse, many new regulations have been established to help protect customers. The General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws in existence (HRW, 2018). The GDPR is a comprehensive privacy regulation covering any organization that operates and has customers in the European Union (EU). While the United States doesn't have comprehensive laws and regulations at the federal level, there are various laws that focus more on the types of privacy and are industry specific, such as HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA (Klosowski, 2021). Three states within the U.S. have enacted comprehensive privacy laws at the state level, which are California (CCPA), Virginia, (VCDPA), and Colorado (ColoPA). Appendix A provides a comprehensive list and description of the privacy laws presented in this section. The increasing number of privacy regulations has added to the complexity of the CPO role in organizations.

Role of a CPO

A CPO is a senior-level executive within an ever-increasing number of global organizations. The primary responsibility of the CPO is the protection of information assets, ensuring the privacy of customers, and managing risk related to information privacy laws and compliance regulations (Pemberton, 2002). This role is ostensibly created in an organization to be a central authority for making privacy decisions and protecting the interests of a company's customers. Any organization that collects and stores customer information should have a single place where knowledge resides about how the information is managed and where policies are established for obtaining and handling online and offline data (Bowcut, 2021).

A CPO is a leader and champion for data privacy within an organization and its customers. The individual interacts and oversees third-party relationships and ensures that data flowing to and from customers, internally via systems, and externally via vendors and following outlined policies and procedures. Privacy policies originate and are overseen by a CPO. The Data Privacy Program for the organization is coordinated and overseen by the CPO. Coordination of an audit of the program, maintaining it, and ensuring the organization is abiding by the program is a key function of their role.

CPOs must also keep up with any changes in privacy laws, advancements in technology, and any operational changes in the company to ensure privacy policies are updated accordingly. Communicating and collaborating with the company's IT department and other C-Suite executives is vital to preventing unauthorized access to the secured data (Kayworth, 2005). Additionally, as a privacy officer, duties include assessing current policies, suggesting modifications, and training new and existing employees on these policies. The CPO must stay informed of changes to privacy laws to ensure that your company's policies reflect current regulations (Sipior and Ward, 2001). Their job is to oversee the implementation of the best possible privacy practices ensuring the privacy of personal information and records so that no legal issues arise.

Methodology

The current research will employ a qualitative methodology using structured interviews to collect data from current CPOs and organizations that do not have a CPO. This will require two data collections among organizations with a CPO and those without. The goal is to identify the roles and characteristics of a CPO based on how current professionals perform their job. We will then conduct interviews with IT

organizations that do not have a CPO to evaluate how the identified roles and responsibilities are allocated to other job roles.

Data Collection

Data will be collected from CPOs and the IT staff of organizations that do not have the CPO role. Based on general recommendations for qualitative interviews, we intend to identify 20 participants for each round of interviews (Marshall et al. 2013). Through networking connections and identifying current CPOs through LinkedIn, we will interview 20-25 current CPOs working in the United States holding the official job title. Our second round of interviews will consist of organizations that do not have a CPO. These organizations are recruited based on current connections with industry and other companies will be identified through networking connections.

Analysis

Using multiple researchers to code the data, we will conduct interrater reliability and triangulation to validate and results and ensure reliability. Our analysis will evaluate how the role of the CPO has evolved due to the growth of technology and the growth of data that is collected. We will then conduct a comparative analysis between companies with a CPO and those without to determine how the roles and responsibilities are distributed without a designated privacy officer. Characteristics of each company will be evaluated along with challenged identified in securing data and complying with regulations to establish a model to help assess the need of a CPO.

Discussion

This research in progress proposes several theoretical and practical implications with recommendations for future research. First, we will identify the expanded roles and responsibilities that current CPOs operate under in modern business. We will identify common characteristics of a CPO to help organizations seeking to add the CPO role to their organization identify the right fit and qualifications. We will also develop a model with a stepwise approach for analyzing an organization's situation and data privacy needs to determine if a CPO is needed. Based on the outcomes identified in this research, several recommendations for future research will be formulated.

Conclusion

This emerging research forum is research in progress with the intention to get feedback that will improve our research design and analysis. Our plan is to further develop the literature review, organize our interview questions, conduct content validity to improve our interview questions, and identify participants prior to the AMCIS conference. Feedback from the conference would be very valuable for improving this research prior to conducting interviews and analyzing the data.

References

ACDS. 2020. "Q & A with Jennifer Barrett Glasgow," *ACDS Newsletter* (2:2), Retrieved from https://www.acds.co/post/qaglasgow

Ashbel, A. 2020. "Data Protection Officer vs Chief Privacy Officer: A Comparison of Two Compliance-Related Roles," *NetApp*, Retrieved from https://cloud.netapp.com/blog/cvo-blg-data-protection-officer-vs-chief-privacy-officer

Bowcut, S. 2021. "How to become a chief privacy officer: A complete career guide," *Cybersecurity Guide*, Retrieved from https://cybersecurityguide.org/careers/chief-privacy-officer/

Brown, J. 2014. "Rise of the Chief Privacy Officer," *Government Technology*, Retrieve from https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html

Clark, S. 2020. "4 Ways a Chief Privacy Officer Can Help Your Company," *Reworked*, Retrieved from https://www.reworked.co/information-management/4-ways-a-chief-privacy-officer-can-help-your-company/

Cloudflare. 2022. "What is Data Privacy?" *Cloudflare*, Retrieved from https://www.cloudflare.com/learning/privacy/what-is-data-privacy/

Coos, A. 2020. "DPO vs. CPO: Compliance Roles at Glance," *Endpoint Protector*, Retrieved from https://www.endpointprotector.com/blog/dpo-vs-cpo-compliance-roles-at-glance/
Edelstein, S. 2018. "Uber Hires Chief Privacy Officer, Data Protection Officer," *The Drive*, Retrieved from https://www.thedrive.com/tech/22265/uber-hires-chief-privacy-officer-data-protection-officer
EDPS. 2022. "The History of the General Data Protection Regulation," *European Data Protection Supervisor*, Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
Glen. 2020. "CISO vs CSO: What Do They Mean?" *CISO Portal*, Retrieved from https://www.ciso-portal.com/ciso-vs-cso-what-do-they-mean/
Hadley, Jr., R. 2018. "The Chief Privacy Officer: A Must Hire in Today's Complex Digital World," *The Compliance & Ethics Blog*, Retrieved from https://complianceandethics.org/the-chief-privacy-officer-a-must-hire-in-todays-complex-digital-world/
HRW. 2018. "The EU General Data Protection Regulation: Questions and Answers," *Human Rights Watch*, Retrieved from https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation
IAPP. 2022. "What is Privacy?" *International Association of Privacy Professionals*, Retrieved from https://iapp.org/about/what-is-privacy/
Kayworth, T., Brocato, L. and Whitten, D. 2005. "What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles," *Communications of the Association for Information Systems* (16), pp. 110-126.
Klosowski, T. 2021. "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," *Wirecutter*, Retrieved from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/
Marshall, J. 2001. "The Emerging CPO - Chief Privacy Officer," *Financial Executive* (17:2), pp. 10.
Pemberton, J. 2002. "Chief Privacy Officer: Your Next Career?" *Information Management Journal* (36:3), pp. 57-58.
Privacy Commissioner. 2020. "What is a privacy officer? Am I required to have a privacy officer?" *Privacy Commissioner*, Retrieved from https://www.privacy.org.nz/tools/knowledge-base/view/179
Salvi, V. 2021. "Data Breaches: A potential dent to brand-customer relationships," *Business Today*, Retrieved from https://www.businesstoday.in/opinion/columns/story/data-breaches-a-potential-dent-to-brand-customer-relationships-307166-2021-09-20
Sipior, J. and Ward, B. 2001. "Cyberliability: is the chief privacy officer the solution?" in *Proceedings of the 9th European Conference on Information Systems*, Bled, Slovenia, pp. 177-187.
von Ogden, J. 2014. "CSO vs. CISO," *CIMCOR*, Retrieved from https://www.cimcor.com/blog/cso-vs-ciso
ZipRecruiter. 2022a. "What Does a Chief Privacy Officer Do," *ZipRecruiter*, Retrieved from https://www.ziprecruiter.com/e/What-Does-a-Chief-Privacy-Officer-Do
ZipRecruiter. 2022b. "What Is a Privacy Officer and How to Become One," ZipRecruiter, Retrieved from https://www.ziprecruiter.com/Career/Privacy-Officer/What-Is-How-to-Become

Appendix A: List of Privacy Laws and Regulations

The appendices were removed due to space limitations.