Privacy Is a Major Concern for Higher Ed: Enter the CPO

Until fairly recently, chief privacy officer (CPO) was a title limited mainly to the private sector. Today, more and more higher education institutions are hiring CPOs to address growing concerns about data collection and privacy on college campuses.

While many administrators might have been reactive to security issues in the past, this growth in CPO positions clearly shows that that time is over. CPOs are expected to craft proactive strategies for data and security concerns. In fact, as new techniques are developed and cyber threats become more common, CPOs are expected to take on responsibilities on par with any other critical C-Suite level role.

The Role of the CPO

The CPO is essentially a senior level executive that handles the private information of an organization, but the role is expanding rapidly, especially in the world of Higher Ed. Some responsibilities include:

- Compliance. Confirming the organization maintains compliance with laws at every level, from local to international regulations. This usually entails record retention and management.
- Campus security. Establishing campus policies and standards and overseeing their enforcement in regard to privacy and data handling.
- Privacy training. Developing competent privacy training for staff and faculty, strategic IT policies, and data governance.
- Enhancing awareness. Educating students and promoting awareness of privacy concerns as well as addressing any inquiries.
- Dealing with security breaches. Investigating privacy breaches and responding accordingly, often in tandem with other campus executives.

Major data breaches make headlines, so CPOs are more important than ever to an organization's operating power. The CPO's influence in higher education exponentially increased over the last decade as information demands grew more complex.

Data management and privacy issues are no longer fringe responsibilities—they're now vital to any industry, and, as an industry, higher education brings with it special challenges. Data security encompasses an organization's networks, governance, partnerships, student and faculty safety, and the ability to function at a commercial level.

CPOs typically work closely with Chief Information Security Officers (CISOs). The CPO determines how a company should manage and protect data, and the CISO will implement those decisions. Security is largely a technical discipline, while privacy relates more to the institution's operations—though it of course relies heavily upon security, as maintaining the privacy of data requires the physical and virtual safety afforded by a competent IT strategy.

CPOs: Expanded Responsibilities and Opportunities

The scope of this position in higher education institutions is rapidly expanding, and while CPOs need to focus on the core responsibility of safeguarding an institution's private information, there are day to day things that a CPO can do to maximize their efficacy on campus. For example:

- Complete regular assessments and effectiveness checks of privacy programs.

- Participate in “sensitive data” inventories and maintain close collaboration with CISOs and data stewards.
- Raise campus awareness of privacy concerns, and publicize their role as CPO by educating students and staff and addressing everyday privacy and security concerns.
- Work to design privacy into IT structures and operations.
- Design targeted, specialized strategies and outline new regulations to help prepare for emergent threats.
-

An established and knowledgeable senior privacy executive is an asset to any higher education institution. The role expanded in light of new challenges, and it will continue to do so as technology and risks evolve. The CPO will soon be the face and the voice of campus strategies in data management, as new advances further change the digital landscape of higher education.