castlight search

We are expert in the recruitment of healthcare's cyber security leadership

The need for stronger cybersecurity is now on most healthcare organizations' radars, more so than even just a few years ago and with data sharing the need for cyber security is even greater. CIOs along with CISOs, privacy officers, and compliance officers, should ensure healthcare organizations have designated privacy or security officer, with a CISO being ideal, and that regular security training takes place for everyone.

Chief Information Security Officer. The CISO needs to understand the technology and the threats well enough to understand what the organization needs to do to protect its system, operations and its information. CISOs must now have knowledge in many areas, and understand just how far data breach repercussions can go. The role has evolved from being focused primarily on the implementation and management of security control technology (firewall, IDS, AV solutions, etc.) to a consultative, business process aware, risk management professional.

Chief Privacy Officer. 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 CDO.

In many cases, the CPO may have grown into the role from within the organization coming from IT, compliance, or HR. CISOs almost always come from IT on the infrastructure side.

Distinguishing between the CISO and the CPO

Policy ownership, as an example

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.

Corporate Compliance Officer establishes and implements an effective compliance program to prevent illegal, unethical or improper conduct. The compliance officer acts as staff to the CEO and Governing Board by monitoring and reporting results of the compliance and ethics efforts of the company and in providing guidance for the Board and senior management team on matters relating to reporting and compliance. The corporate compliance officer, together with the Corporate Compliance Committee, is authorized to implement all necessary actions to ensure achievement of the objectives of an effective compliance program.