Compliance

Why it's a bad idea to combine the CISO and DPO roles

Darren Wray October 28, 2022

Today's columnist, Darren Wray of Donnelley Financial Solutions, points out that the data protection officer differs from the CISO in that they are charged under regulations such as European Union's GDPR to make sure data doesn't get used for marketing purposes. (Photo by Carl Court/Getty Images)

Inflation and a looming recession are prompting many companies to examine their bottom lines to see if and where they can cut costs. Often, this includes streamlining and laying off staff to increase efficiencies and eliminate redundancies. For companies that have both a chief information security officer (CISO) and a data protection officer (DPO), it's natural to ask: Can we combine these roles?

A better question for companies: Are we prioritizing — and funding — data security and data privacy? With both cyber threats and regulations on the rise, it's now critical to do so. If managed well, proper security and data privacy funding could propel companies to thrive through a recession and beyond.

Cut security or privacy? Proceed with caution

For companies that handle sensitive or personal identifiable information (PII)— financial services organizations, retailers, healthcare, and enterprises — laying off the CISO or DPO could make for a bad outcome, especially when PII stands more vulnerable and at risk than ever.

To many people, the roles of the CISO and DPO seem similar, and it's not uncommon for companies to combine them into a single job in some parts of the world. It's simply a case of semantics, right? Not at all. While they both deal with the protection of data and operations, each one has different approaches and requirements, not to mention regulations and governance.

Let's take a look at their respective roles:

The CISO, or security officer, protects an organization's data and operations from harm. This includes the theft of data or assets, or the disruption of business operations, perhaps caused by a data breach affecting employees, customers, and possibly the entire supply chain. As such, a security officer prevents data from getting into the wrong hands and helps to keep critical business systems and processes running in the face of attempts to breach or disrupt them.

At first glance, the role of a DPO may seem similar to the CISO: keep personal information safe and ensure it's used for correct and lawful purposes. But there are subtle, yet important differences. The DPO must ensure that data does not get misused. Under data privacy and protection legislation in most parts of the world, like the General Data Protection Regulation (GDPR) across the EU, just because a business collects customer information, it does not have the right to use it for other purposes, such as marketing.

CISO and DPO: The great divergence

DPO's are also responsible for releasing personal information outside of the organization from time-to-time, and to delete information held by the business at the request of someone outside of the business. For example, when a right of access (known as a DSAR in many parts of the world) or a right to erasure request is made, the DPO's team will assess this request to ensure it's a legal and legitimate one, and that the person requesting the data is who they say they are.

In the case of a DSAR, a DPO will redact the personal information of people other than the requestor and redact any confidential company information from the data and documents before the information gets sent to the requestor. It's an arduous job and can take thousands of person hours a year to achieve without a software solution tool. For erasure requests, the same initial checks are made. Assuming that they all pass, the information relating to the requestor gets redacted from documents and deleted from databases, despite potential CISO objection or as dictated by other parts of the organization.

Put simply, security and privacy go hand in hand, yet combining CISO and DPO roles can be a bad idea because they are often in — healthy — opposition.

If a company still wants to do it, proceed with caution. With security and privacy now board-level issues, companies really need to put the decision to combine these roles on the docket during the next board meeting.

Darren Wray, executive of data protect solutions, part of Donnelley Financial Solutions (DFIN)

Darren Wray