Pitfall3: Failure to define who owns responsibility for the data

Bookmark this page

Even when aware of the need for data security, many companies have no one specifically responsible for protecting sensitive data. This situation often becomes apparent during a data security or audit incident when the organization is under pressure to find out who is actually responsible. Top executives may turn to the chief information officer (CIO), who might say, “Our job is to keep key systems running. Go talk to someone in my IT staff.” Those IT employees may be responsible for several databases in which sensitive data resides and yet lack a security budget.

Typically, members of the chief information security officer (CISO) organization aren’t directly responsible for the data that’s flowing through the overall business. They may give advice to the different line-of-business (LOB) managers within an enterprise, but, in many companies, nobody is explicitly responsible for the data itself. For an organization, data is one of its most valuable assets. Yet, without ownership responsibility, properly securing sensitive data becomes a challenge.

Solution: Hire a CDO or DPO dedicated to the well-being and security of sensitive and critical data assets In complex IT environments, it’s critical to account for data in the following locations

- Shared across business units
- Located in hybrid multicloud infrastructures
- Stored on mobile devices

A chief data officer (CDO) or data protection officer (DPO) can handle these duties. In fact, companies based in Europe or doing business with European Union data subjects face GDPR mandates that require them to have a DPO. This prerequisite recognizes that sensitive data—in this case personal information—has value that extends beyond the LOB that uses that data. Additionally, the requirement emphasizes that enterprises have a role specifically designed to be responsible for data assets.

Consider the following objectives and responsibilities for choosing a CDO or DPO:

- Technical knowledge and business sense: Assess risk and make a practical business case that nontechnical business leaders can understand regarding appropriate security investments.
- Strategic implementation: Direct a plan at a technical level that applies detection, response and data security controls to provide protections
- Compliance leadership: Understand compliance requirements and know how to map those requirements to data security controls so that your business is compliant.
- Monitoring and assessment: Monitor the threat landscape and measure the effectiveness of your data security program.
- Flexibility and scaling: Know when and how to adjust the data security strategy, such as expanding data access and usage policies across new environ-ments by integrating more advanced tools.
- Division of labor: Set expectations with cloud service providers regarding service-level agreements (SLAs) and the responsibilities associated with data security risk and remediation.
- Data breach response plan: Finally, be ready to play a key role to devise a strategic breach mitigation and response plan.

Ultimately, the CDO or DPO should lead in fostering data security collaboration across teams and throughout your enterprise, as everyone needs to work together to effectively secure corporate data. This collaboration can help the CDO or DPO oversee the programs and protections your organization needs to help secure its sensitive data

Previous Next