WINSTON & STRAWN LLP

ARTICLE

Corporate Compliance Strategies To Protect Data

NOVEMBER 2020

This article was originally published in the November 2020 issue of CISO Mag. *Any opinions in this article are not those of Winston & Strawn or its clients. The opinions in this article are the author's opinions only.*

The pandemic has pushed the corporate workforce to remote locations, which has resulted in increased risk to corporate data. As corporations rise to the challenge of responding to this risk, compliance officers, CISOs, and leaders should look to revamp disjointed and siloed approaches to protecting corporate data. The past few years have seen a notable expansion of trade secret laws resulting from a new federal trade secret act in the U.S., the passage of stricter trade secret regimes in Asia, and the harmonization of trade secret protection in Europe with the EU trade secret directive. With these new laws has come a noticeable uptick in trade secret civil and criminal cases. Like traditional compliance risks, theft or loss of information can lead to loss of valuable R&D, business disruption, loss of competitive advantage, reputational damage, and – if an employee improperly uses a third-party's trade secrets – costly civil or criminal litigation. While ransomware, hacking, and phishing schemes often get the most news coverage, insider theft represents the vast majority of data loss.

To learn more about what companies need to be doing to safeguard sensitive information, read the full article here (subscription required).

1 Min Read

Related Locations

Chicago | Houston

Related Topics

Compliance Programs | Privacy and Data Security | COVID-19

Related Capabilities

Privacy & Data Security

Compliance Programs

Trade Secrets, Non Competes & Restrictive Covenants

Related Regions

North America

Related Professionals

Steven Grimes

© 2025 Winston & Strawn LLP.