WINSTON & STRAWN LLP

BLOG

Code42 Report Finds Companies Are Not Sufficiently Combatting Risk of Insider Data Threats

JANUARY 14, 2020

Code 42 recently released its 2019 Global Data Exposure Report which identified employees as being one of the greatest threats to a company's ability to protect its valuable data and found that companies are not sufficiently addressing and mitigating the risk of this threat. The report warns companies: "If insider threat data loss is not top of mind for your organization, it should be."

Code42's survey of 1,028 information security leaders and 615 business decision-makers who oversee cybersecurity solutions found, among other things:

- **Employees bring data from prior employers**: 63% of respondents admitted to taking data from their past employers and bringing it into the current business.
- **Companies are not sufficiently preventing infiltration of others' secrets**: Even though 57% of information security leaders believed employees have infiltrated data from other companies, 27% of information security leaders said they do not monitor data new employees bring into the company.
- **Employees falsely believe they own company data**: 71% of respondents responded that it is "not just corporate data, it's my work – and my ideas."
- **Decision-makers are using unapproved sharing mechanisms**: 43% of business decision-makers admitted using *personal* email to send company files and collaborate with colleagues and 31% admitted using social media platforms to do so.
- **Employees disregard best practices and required protocols**: 77% of information security leaders agreed that the "most significant" risk to an organization is employees doing their job tasks how they want while not regarding data security protocols and rules, yet according to Code42 "employees tend to operate however they please to get their jobs done."

One major takeaway from Code42's report is that preventative solutions, such as data loss prevention software, are not enough. In fact, 69% of respondents said their organizations had suffered a data breach or loss due to an insider even though they had a preventative solution, like DLP, in place at the time.

TIP: Each company needs to approach data and trade secret protection thoughtfully, proactively, and in a nuanced way tailored to the company's specific secret, business needs, and risk profile and must avoid having false sense of security based on the use of data loss prevention software, training, agreements, or other mechanisms.

2 Min Read

Author

Steven Grimes

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Compliance Programs

Related Regions

North America

Related Professionals

Steven Grimes

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.