WHITEPAPER

3 Key Concerns CISOs Have About Cyber Insurance

LUCIDUM

With the ever-revolving threat landscape and the potential financial and reputational damage that can be caused by a data breach, there are some key concerns CISOs have as they evaluate their needs for Cyber Insurance:

01.

Cost of cyber insurance: According to the Council of Insurance of Insurance Agents and Brokers, there was an average of 27.6% increase in premiums during Q3 2021 atop a rise of 25% in the previous quarter. The cost of cyber insurance is typically based on factors such as the size of the organization, the type of data being protected, and the potential damages that could be caused by a breach. CISOs need to carefully weigh the cost of cyber insurance against the potential benefits it could provide in the event of a breach.

02.

Overage limits: It is important for CISOs to make sure that the coverage limits of their cyber insurance policy are sufficient to cover the potential costs of a breach. Cyber insurance policies typically include coverage limits for specific types of damages, such as data restoration costs, legal fees, and reputational damage. CISOs need to ensure that their coverage limits are high enough to cover the cost of a breach, and that there are no gaps in coverage that could leave their organization exposed.

03.

Eligibility: To be eligible for cyber insurance, a CISOs company must keep track of who has access to different files and resources. This process, also referred to as User Lifecycle Management, ensures that their employees have all the permissions necessary to complete their tasks - but no unnecessary permissions that pose a security risk.

CISO's Know Managing User Access Rights from One Central Platform Greatly Reduces Risks: Managing user access rights from one central platform not only helps CISOs qualify for insurance, but is also a key step for many industry-specific compliance standards. Compliance regulations that directly specify or greatly benefit from an identity and access management solution include the Sarbanes-Oxley Act (SOX Compliance) in the financial industry, the Health Insurance Portability and Accountability Act (HIPAA) and TIXAX certification in the automotive industry. It is also a component of the ISO 27001 information security standard.

Learn more at www.lucidum.io

LUCIDUM