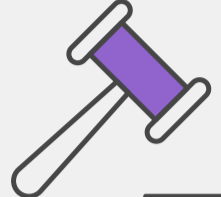


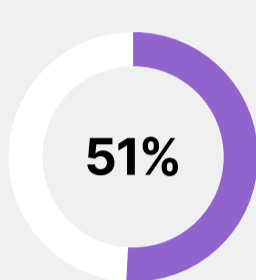
2024 Cybersecurity Skills Gap Global Research Report

Executive Summary

When it comes to cybersecurity in 2024, the stakes are high for organizations. Breaches continue to take a financial toll—and senior leaders are penalized when they happen. In response, organizations are focusing on a three-pronged approach to cybersecurity that combines training, awareness, and technology.



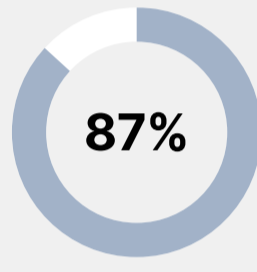
Corporate leaders are being held accountable



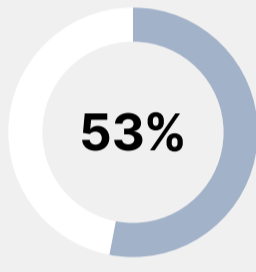
51% of respondents say directors or executives have faced fines, jail time, or loss of employment/position following a cyberattack.



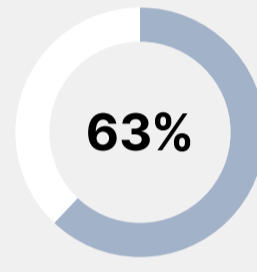
Breaches consume precious time and money



87% of organizations have experienced one or more security breaches in the last 12 months.



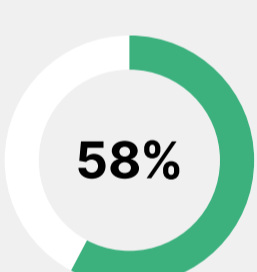
53% of organizations suffered breaches that cost more than \$1M.



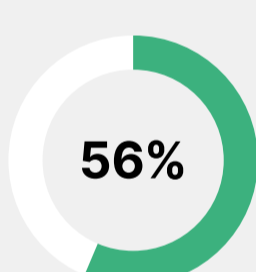
63% of organizations say it took longer than a month to recover.



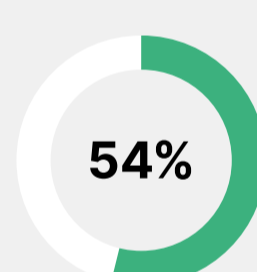
IT leaders closely rank the main three causes of breaches



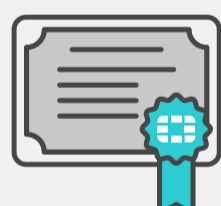
58% of breaches are caused by lack of cybersecurity skills and training.



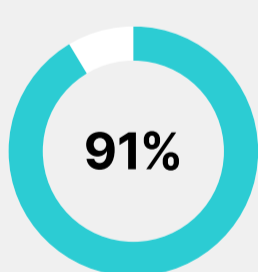
56% of breaches point to insufficient organizational or employee security awareness.



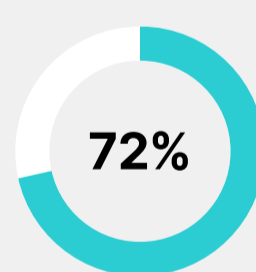
54% of breaches are due to lack of cybersecurity products.



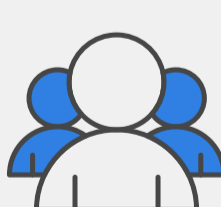
Candidates with certifications stand out



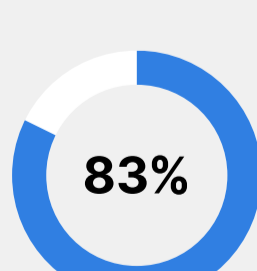
91% of organizations prefer to hire candidates with certifications.



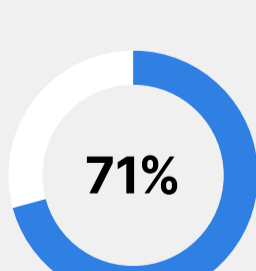
72% of organizations report it is hard to find people with certifications.



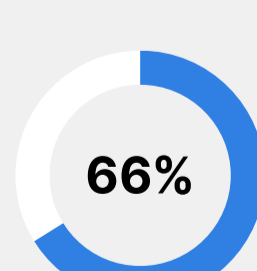
Organizations may be overlooking candidates from underrepresented backgrounds



83% of companies have set diversity hiring goals for the next few years.



71% of companies require four-year degrees.



66% of companies hire only candidates with traditional training backgrounds.

[READ THE FULL REPORT](#)