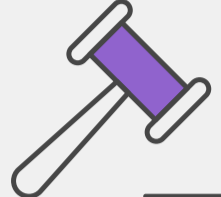


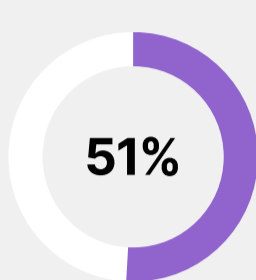
2024 Cybersecurity Skills Gap Global Research Report

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.



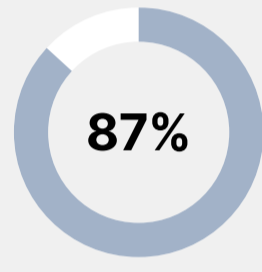
Corporate leaders are being held accountable



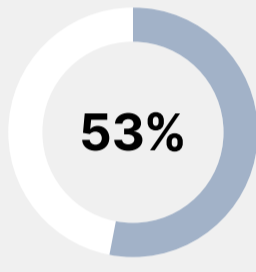
of respondents say directors or executives have faced fines, jail time, or loss of employment/position following a cyberattack.



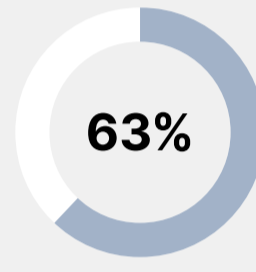
Breaches consume precious time and money



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



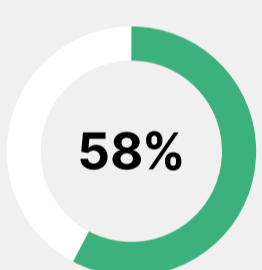
of organizations suffered breaches that cost more than \$1M.



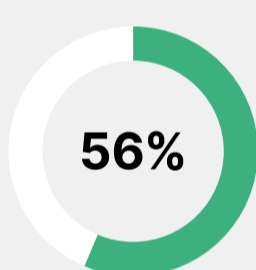
of organizations say it took longer than a month to recover.



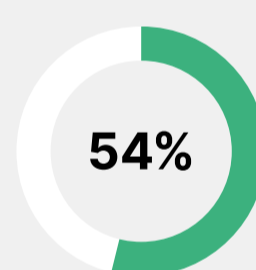
IT leaders closely rank the main three causes of breaches



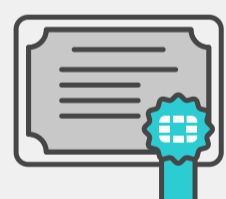
caused by lack of cybersecurity skills and training.



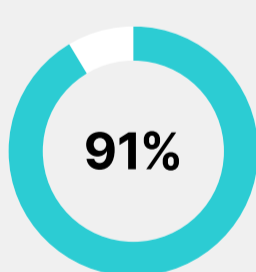
point to insufficient organizational or employee security awareness.



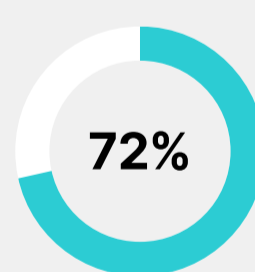
due to lack of cybersecurity products.



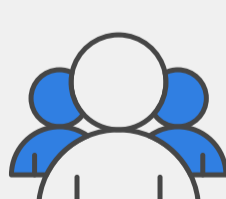
Candidates with certifications stand out



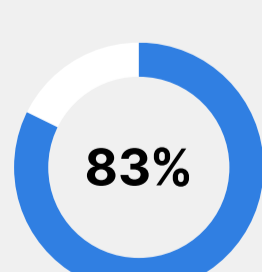
of organizations prefer to hire candidates with certifications.



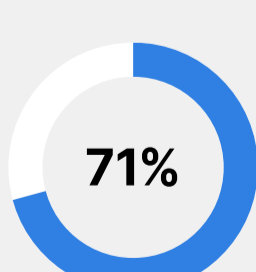
of organizations report it is hard to find people with certifications.



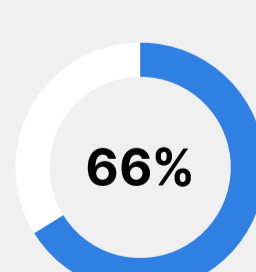
Organizations may be overlooking candidates from underrepresented backgrounds



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



of companies require four-year degrees.



of companies hire only candidates with traditional training backgrounds.

[READ THE FULL REPORT](#)