

EUROPEAN REGION

# State of Cybersecurity in 2023 and Beyond

More than 550 security leaders share their insights on the latest cybersecurity threat landscape, hiring challenges and opportunities, budgets, and more in ISACA's ninth annual State of Cybersecurity study. These findings are key to helping shape action plans, as organizations continue to grapple with a complicated threat landscape and understaffed teams.



## Cyberattack Landscape



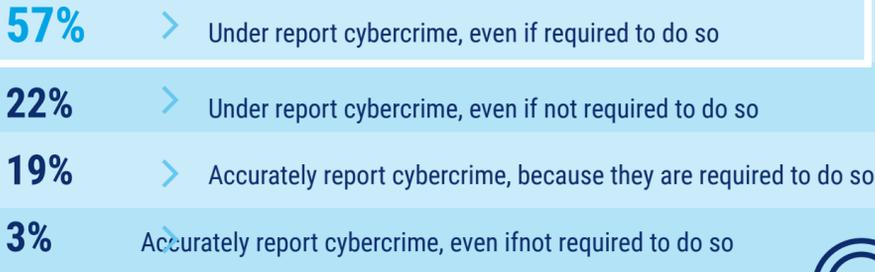
NEARLY **52%**

of organizations are experiencing **MORE CYBERATTACKS** than last year.



**78%**

say most organizations **UNDER-REPORT** cyberattacks.



## TEAMS REMAIN UNDERSTAFFED



**62%** of cybersecurity leaders say their teams are understaffed.

**41%** have a high degree of confidence in their cybersecurity team's ability to detect and respond to cyber threats.

## DESPITE COOLING JOB MARKET, Cybersecurity Talent Is Still in Demand



**47%**

### NON-ENTRY LEVEL POSITIONS:

47% of respondents have job openings for these roles



**20%**

### ENTRY-LEVEL POSITIONS:

20% have job openings for these roles



**68%**

of cybersecurity leaders say they have difficulty retaining qualified cybersecurity professionals

## TOP FIVE

## Technical Skills Needed Now

- 50%** Cloud computing
- 49%** Identity and access management
- 46%** Incident response
- 45%** Data protection
- 37%** DevSecOps

## TOP 5 SOFT SKILLS CYBERSECURITY CANDIDATES SHOULD HOLD:



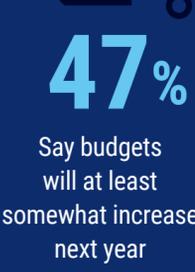
## TOP 3 WAYS Employers Determine a Candidate Is Qualified



## Certification Is a Path to Success



## 2024 OUTLOOK



For full study results, download the free State of Cybersecurity 2023 report at [www.isaca.org/state-of-cybersecurity-2023](http://www.isaca.org/state-of-cybersecurity-2023)

SPONSORED BY : Adobe