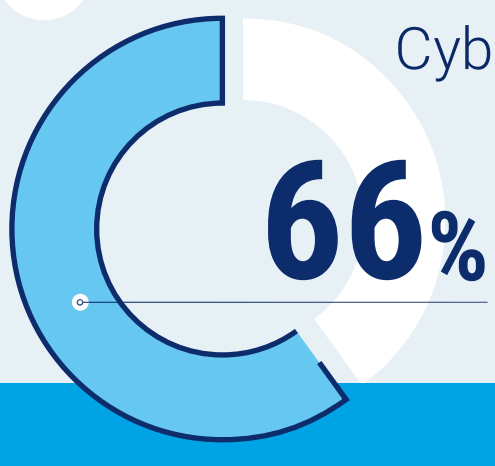
ISACA

GLOBAL EDITION

State of Cybersecurity
2024 and Beyond

The majority of cybersecurity professionals say their roles are increasingly stressful—in large part due to a threat landscape that continues to become more complex. ISACA, a global professional association advancing trust in technology, surveyed more than 1,800 cybersecurity professionals to examine the state of cybersecurity in 2024 and beyond, from skills gaps and hiring plans to threats and budgets. For full results, visit www.isaca.org/state-of-cybersecurity-2024.

Cybersecurity Professionals Are Stressed



66% say their role is **more stressful** now than five years ago

TOP REASONS FOR INCREASED STRESS:

1. Threat landscape is increasingly complex. (81%)
2-4. Budget is too low. (45%)
Hiring/retention challenges have worsened. (45%)
Staff are not sufficiently trained/skilled. (45%)
5. Cybersecurity risks are not prioritized. (34%)

"Employers should home in on occupational stress for their digital defenders. Take the opportunity to explore ways to support staff before burnout and attrition occur. Employees want to feel valued. As the leadership adage goes, take care of your people and they'll take care of you."

JON BRANDT • *Director of Professional Practices and Innovation, ISACA*

Cybersecurity Job Openings Are Declining

Though **57% OF ORGANIZATIONS** say their cybersecurity teams are understaffed, hiring has slightly slowed:

38% of organizations have no open positions, compared to **35% LAST YEAR**.

46% of organizations have non-entry-level cybersecurity positions open, compared to **50% LAST YEAR**.

18% have entry-level positions open, compared to **21% LAST YEAR**.

TOP TWO FACTORS FOR DETERMINING QUALIFIED CANDIDATES:

1. **73%** Prior hands-on experience
2. **38%** Credentials held

Most Common Skill Gaps

1. **51%** Soft skills, especially communication, critical thinking and problem-solving
2. **42%** Cloud computing

TOP REASONS

Cybersecurity Professionals Leave Their Jobs

55% of respondents have had difficulties retaining qualified cyber candidates.

The most common reasons for leaving are:

- **50%** Recruited by other companies (down 8 points from 2023)
- **50%** Poor financial incentives
- **46%** Limited promotion and development opportunities
- **46%** High work stress levels

Budgets Are Underfunded While Threats Increase

51% say cyber budgets are underfunded (up from 47% in 2023).

ONLY 37% expect budgets will increase in the next year.

38% ARE EXPERIENCING INCREASED CYBERSECURITY ATTACKS compared to 31% one year ago.

TOP ATTACK VECTORS:

1. **19%** Social engineering
2. **13%** Malware
3. **11%** Unpatched system Denial of Service (DoS)

ONLY 40% have a high degree of confidence in their team's ability to detect and respond to cyber threats.

NEARLY HALF (47%) expect a cyberattack on their organization in the next year.

Cybersecurity Needs to Be Prioritized

ONLY 56% say their board has adequately prioritized organizational cybersecurity.

For full study results, download ISACA's free State of Cybersecurity 2024 report at www.isaca.org/state-of-cybersecurity-2024

SPONSORED BY : Adobe