

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—including 413 in Europe—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

68% say their role is **more stressful** now than five years ago

TOP REASONS FOR INCREASED STRESS:

- 1 Threat landscape is increasingly complex. (79%)
- 2-4 Hiring/retention challenges have worsened. (47%)
Budget is too low. (45%)
Staff are not sufficiently trained/skilled. (40%)
- 5 Cybersecurity risks are not prioritized. (32%)

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 **61% OF ORGANIZATIONS** say their cybersecurity teams are understaffed, hiring has slightly slowed:



TOP TWO FACTORS FOR DETERMINING QUALIFIED CANDIDATES:

- 1 **72%** Prior hands-on experience
- 2 **28%** Credentials held

Most Common Skill Gaps

- 1 **52%** Soft skills, especially communication, critical thinking and problem-solving
- 2 **40%** Cloud computing

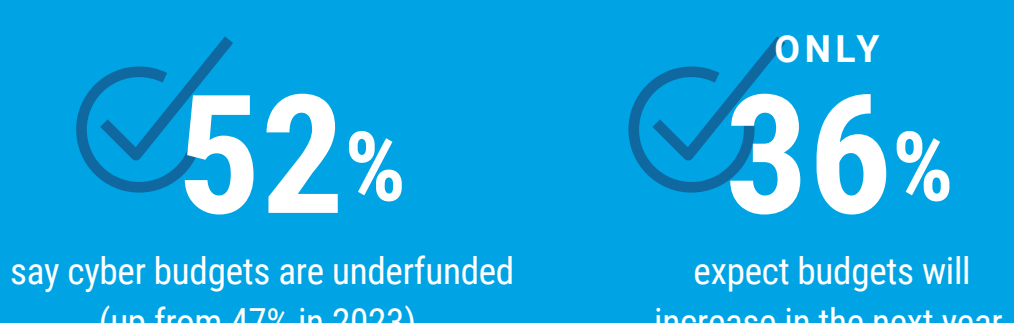
TOP REASONS

Cybersecurity Professionals Leave Their Jobs

55% of respondents have had difficulties retaining qualified cyber candidates. The most common reasons for leaving are:



Budgets Are Underfunded While Threats Increase



41% ARE EXPERIENCING INCREASED CYBERSECURITY ATTACKS compared to 31% one year ago.

TOP ATTACK VECTORS:

- 1 **16%** Social engineering
- 2 **13%** Unpatched system
Denial of Service (DoS)
- 3 **12%** Malware



Cybersecurity Needs to Be Prioritized

ONLY 51% 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**