

# State of Cybersecurity

2025-2026

ISACA surveyed more than 3,800 cybersecurity professionals to determine the state of cybersecurity—from staffing and skills gaps to budgets, threats, and AI use and involvement. Full results are available at [www.isaca.org/state-of-cybersecurity](http://www.isaca.org/state-of-cybersecurity).



## Stress on the Rise

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

**47%**  
High stress is the top reason for attrition

**63%**  
**TOP STRESSOR:** Complex threat landscape

## Staffing Challenges Persist

**55%**  
say their cyber teams are **UNDERSTAFFED**

**65%**  
have **UNFILLED** cybersecurity positions

**38%**  
say it takes **3-6 MONTHS TO HIRE** for entry-level roles, and 39% say the same for non-entry-level roles

### SKILLS GAPS:

Soft Skills, Adaptability and Hands-on Experience in High Demand



**59%** **#1 GAP** Soft skills

### TOP SOFT SKILLS NEEDED:

- 1  **57%** Critical thinking
- 2  **56%** Communication
- 3  **47%** Problem-solving

**Adaptability** is the top qualification factor (61%), with hands-on experience closely following (60%).

### WORKFORCE TRENDS:

Technical Pros in High Demand

**70%**  
expect demand for **TECHNICAL CONTRIBUTORS** to rise

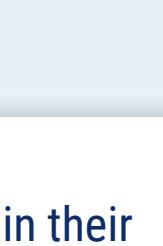
**50%**  
of organizations **STRUGGLE TO RETAIN** cyber talent

**44%**  
say that more than half of their cyber staff **STARTED IN THE FIELD**; 46% say more than half transitioned from other roles.



**ONLY 27%** believe university grads are **well-prepared**

### TOP SKILLS/KNOWLEDGE GAPS IN NEW GRADS:

- 1  **43%** Incident response
- 2  **39%** Data security
- 3  **39%** Threat detection and response technologies
- 4  **39%** Identity and access management

## Cybersecurity Teams Increasingly Involved in AI

### TOP USES OF AI IN SECURITY OPERATIONS:

- 1  Threat detection (32%)
- 2  Endpoint security (30%)
- 3  Routine task automation (28%)

Cybersecurity involvement in AI policy is significantly increasing:

**47%** helped develop AI governance (up from 35%)

**40%** involved in AI implementation (up from 29%)

As cybersecurity threats evolve and stress levels rise, leaders must prioritize both technical resilience and team well-being. Investing in soft skills development, streamlining hiring processes, and involving cybersecurity teams in AI governance are no longer optional—they're strategic imperatives. With budget optimism waning and attacks growing more sophisticated, now is the time to align cyber strategy with business goals, advocate for sustainable funding, and foster a culture that values adaptability, collaboration and continuous learning.

For full study results, download ISACA's free State of Cybersecurity 2025 report at [www.isaca.org/state-of-cybersecurity](http://www.isaca.org/state-of-cybersecurity).