ISC2
RESEARCH

2026 AI Survey:

Rethinking AI's Impact on Cybersecurity Roles

Contents

Intro / Methodology

There continues to be considerable discussion among professionals and hiring managers about how artificial intelligence (AI) is reshaping the cybersecurity profession. From AI-powered security operations platforms and automated threat intelligence tools to generative AI assistants that help analysts investigate alerts and write code, AI is becoming deeply embedded in the daily workflows of cybersecurity professionals across virtually every discipline.

Frequent conversations center on the idea that AI is freeing up time for cybersecurity professionals to focus on more strategic tasks, all while potentially reducing the need for entry-level roles. Many repetitive, time-consuming, and administrative tasks including alert triage, log analysis, report generation, vulnerability prioritization and basic threat hunting are increasingly being performed or accelerated by AI-powered tools. Many of these tasks have traditionally formed part of entry- and junior-level roles.

To gauge the real impact AI is having on the cybersecurity profession, in May 2026 ISC2 conducted a survey of 856 cybersecurity professionals who use AI in their roles. We asked participants questions about how AI is changing the time they spend on various security tasks, their perspectives on how entry-level roles may be evolving, whether AI is affecting their workplace-related stress and more.

Shifts in Time Allocation

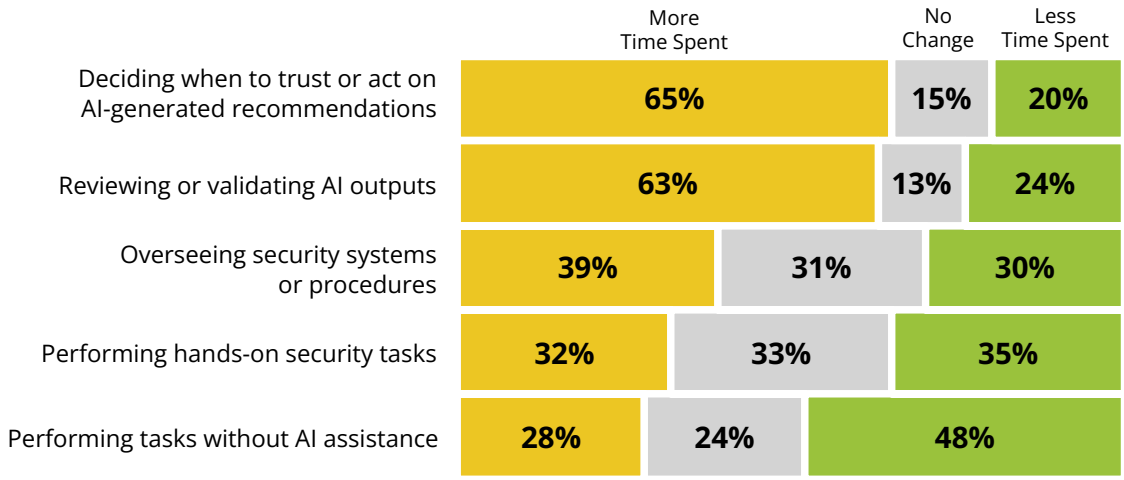
Over the past year, the greatest change in time spent on several security tasks points to the importance of human judgment and decision-making in an AI-enabled environment. Approximately two-thirds of participants spent more time deciding when to trust or act on AI-generated recommendations (65%) and reviewing or validating AI outputs (63%). This is an important measure, as the volume of time and effort being put into validation follows on from other research that has revealed an increasing problem for organizations, where users are acting on AI recommendations without validating them first. For instance, **data from KPMG and the University of Melbourne** in 2025 suggested that two thirds (66%) of general employees – not just cybersecurity professionals – relied on AI-generated output without verifying its accuracy, leading to mistakes in work output for 56% of users.

The time spent on traditional human-led security tasks is also being impacted by AI.

The responses divided into nearly equal percentages, with just over a third noting they spend less time (35%) doing hands-on tasks, while 32% reported spending more time on hands-on tasks and 33% reported no change in their time spent on hands-on tasks due to AI. Results were similar for time spent overseeing security systems or procedures – 30% reported they are spending less time overseeing, 39% reported more time and 31% reported no change to their time spent overseeing due to AI.

In addition to this, nearly half of participants (48%) said that less of their time is now spent working on tasks that don't involve AI assistance.

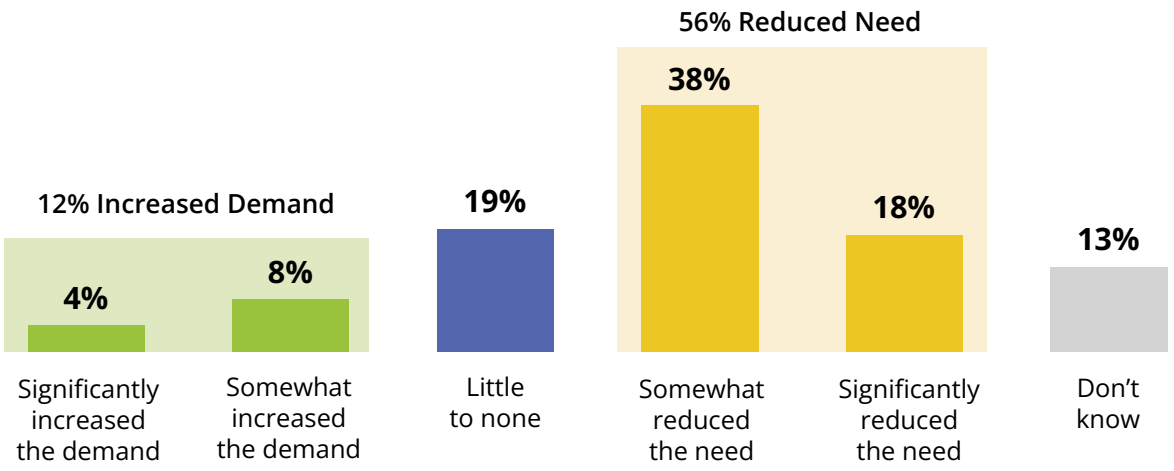
How AI has Changed Time Spent on Security Activities Over the Past Year



Impact on Entry-Level Roles

AI is also reshaping perceptions of early-career roles within cybersecurity. The majority of participants (56%) said that AI has somewhat or significantly reduced the need for entry-level positions over the past year. On the other hand, nearly one in five (19%) reported little to no impact of AI on entry-level roles and 12% said AI has increased the need for these roles. However, 13% were unsure, signaling ongoing uncertainty about how these roles have evolved.

Impact of AI on Entry-Level Cybersecurity Roles in the Past Year



Learning and Skills Development

Over half of participants (53%) believe that AI is creating **new** types of entry-level roles, and nearly half (48%) said AI has made them feel more **optimistic** about their long-term careers in cybersecurity. These findings suggest that traditional early-career roles and the volume of opportunities are not necessarily narrowing, but perhaps evolving, **echoing findings from the most recent ISC2 Cybersecurity Workforce Study.**

Perceptions Split on Hands-on Learning but Need for Fundamentals Remains High

"Many Cybersecurity Professionals are Optimistic about AI."

Many Cybersecurity Professionals are Optimistic about AI

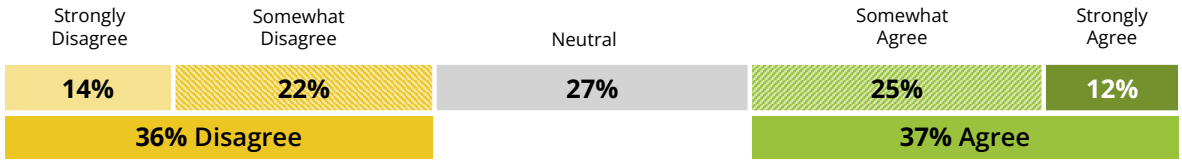
"AI makes me more optimistic about my long-term career in cybersecurity."

Participants were nearly evenly split on whether they believe AI has reduced hands-on learning opportunities in their workplace, with 37% saying it has and 36% saying it has not.

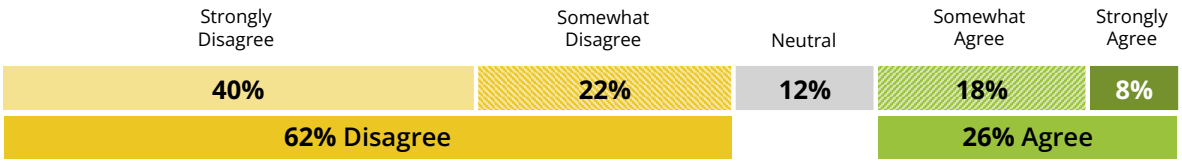
In contrast, nearly two-thirds (62%) do not believe that AI has reduced the need for foundational cybersecurity skills, compared to just 26% who say it has. These findings underscore the continued importance of core technical knowledge and validating foundational competence through education and certification. This is the case, even as AI tools become more prevalent in day-to-day work.

Perceptions Split on Hands-on Learning but Need for Fundamentals Remains High

"AI has reduced hands-on learning opportunities in my workplace."



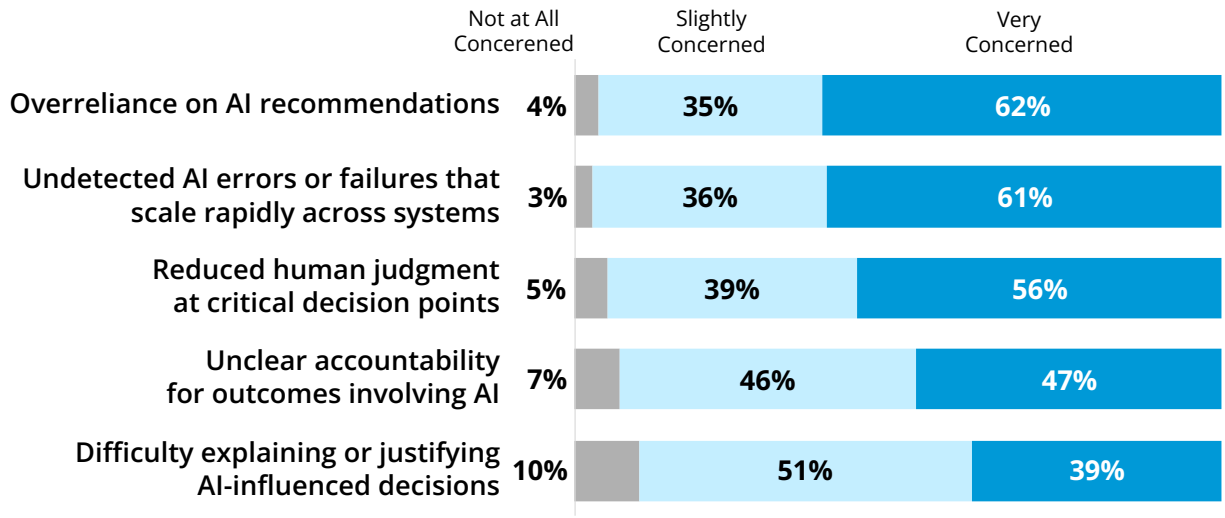
"AI has reduced the need for foundational cybersecurity skills in the cybersecurity profession."



Concerns and Risks

Nearly every participant expressed some level of concern about potential impacts of more autonomous or self-directed AI systems in security operations. The highest levels of concern cited by participants were regarding over-reliance on AI recommendations (62%) and undetected errors that could scale rapidly across systems (61%). Many were also very concerned about reduced human judgment at critical decision points (56%), unclear accountability for outcomes involving AI (47%) and the difficulty of explaining or justifying AI-influenced decisions (39%).

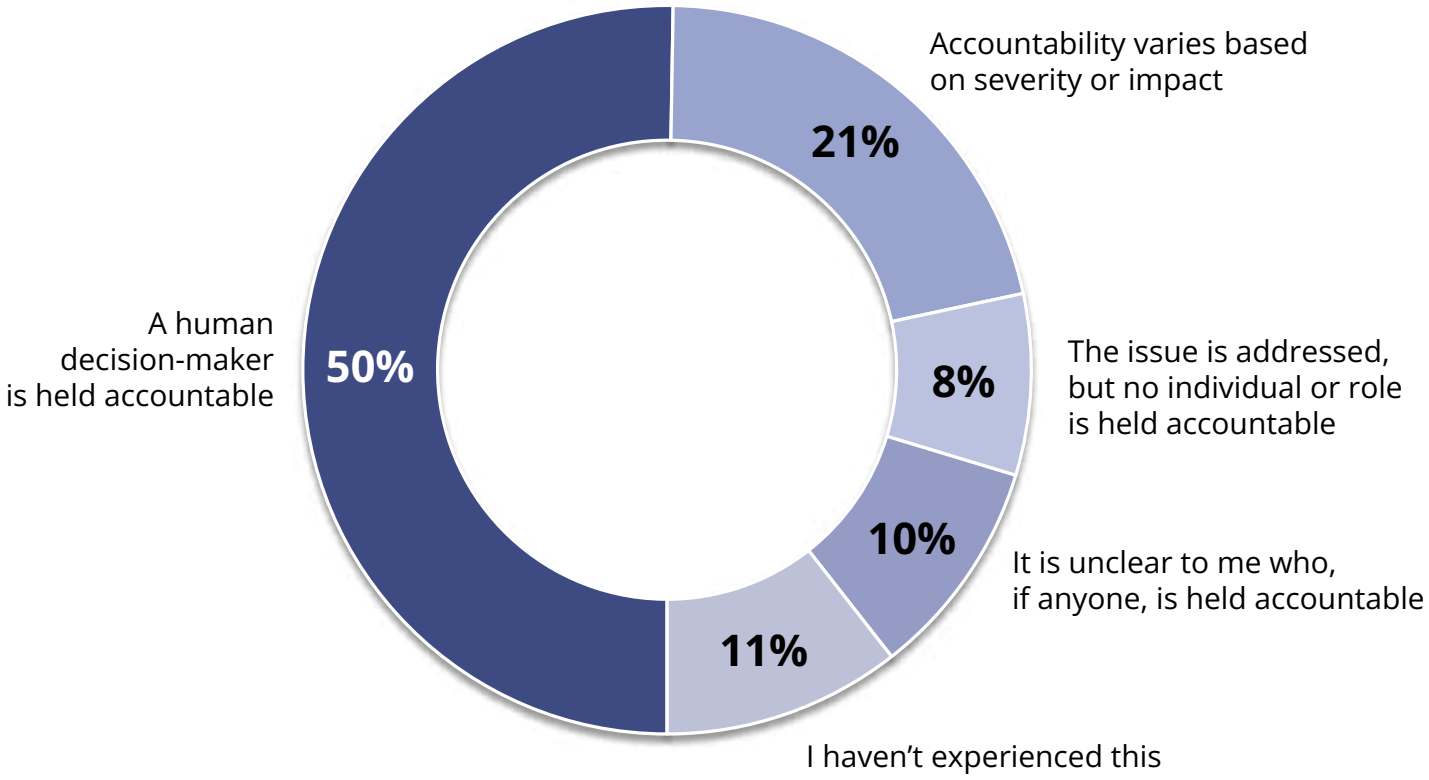
Level of Concern Around Autonomous AI in Cybersecurity



Accountability and Decision-Making Pressure

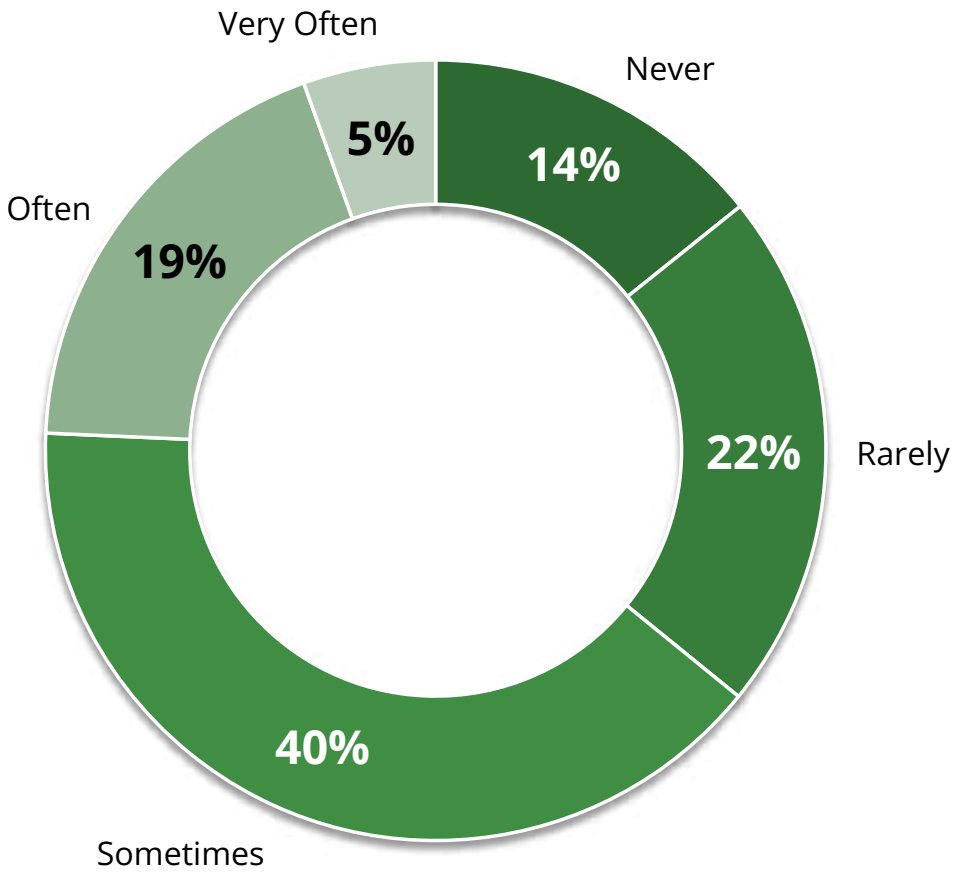
When AI-recommended actions lead to incorrect outcomes, half of participants (50%) said that human decision-makers are ultimately held accountable at their organization. Another 21% said accountability varies depending on the severity of the issue, while others reported ambiguity (10%) or a lack of clear ownership (8%) when AI recommendations are incorrect. Just over 10% have not encountered AI recommendations leading to incorrect outcomes yet, which means that 9 out of 10 (89%) have experienced AI recommendations that lead to incorrect outcomes at their organizations.

Accountability When AI-Recommended Actions Lead to Incorrect Outcomes



Participants' concerns about AI-recommended outputs above appear justified, as many have been asked to act on AI-generated outputs without fully understanding how those outputs were produced. Nearly a quarter (24%) said they are expected to act on AI-generated security outputs often or very often. An additional 40% said they are expected to do this only sometimes. Over a third (36%) of participants said that they are never or rarely asked to act on AI-generated outputs this way.

Expectation to Act on AI Security Outputs Without Understanding Their Origins

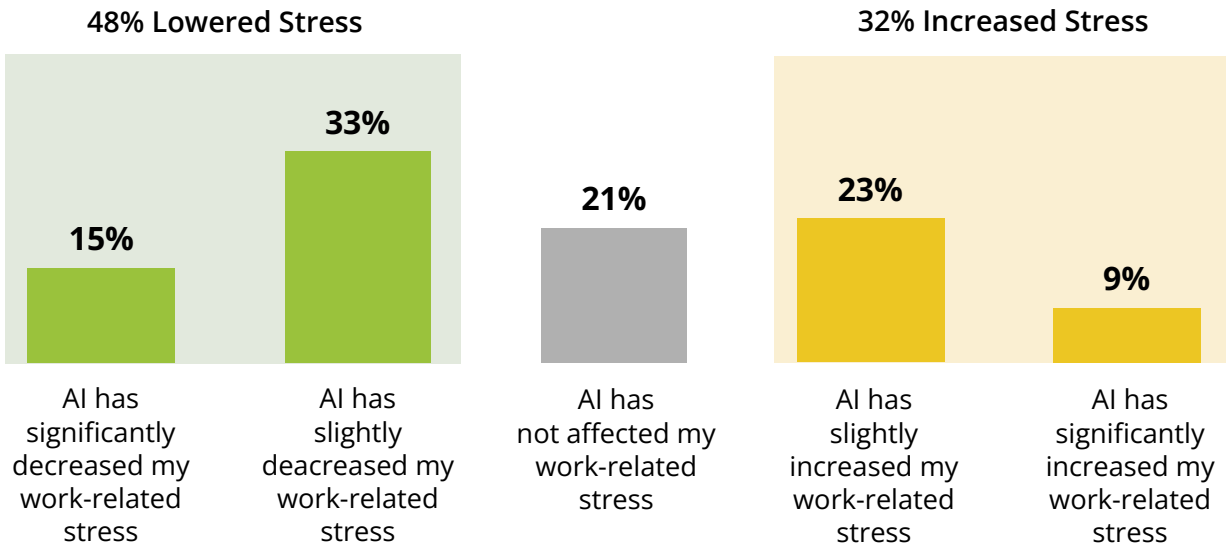


Impact of AI on Work-Related Stress

AI is increasingly being promoted as a tool that can make cybersecurity professionals more productive, efficient and effective. Teams are being encouraged, or required, to incorporate AI-powered tools into their daily activities. While these technologies offer significant benefits, their rapid adoption is also creating a source of workplace stress.

However, the impact of AI on work-related stress is nuanced. At first glance, the overall direction skews positive: Nearly half of participants (48%) reported that using AI has **decreased** their work-related stress over the past year. About a third (32%) said AI has **increased** their work-related stress, and another 21% reported no change in how AI impacted their stress levels.

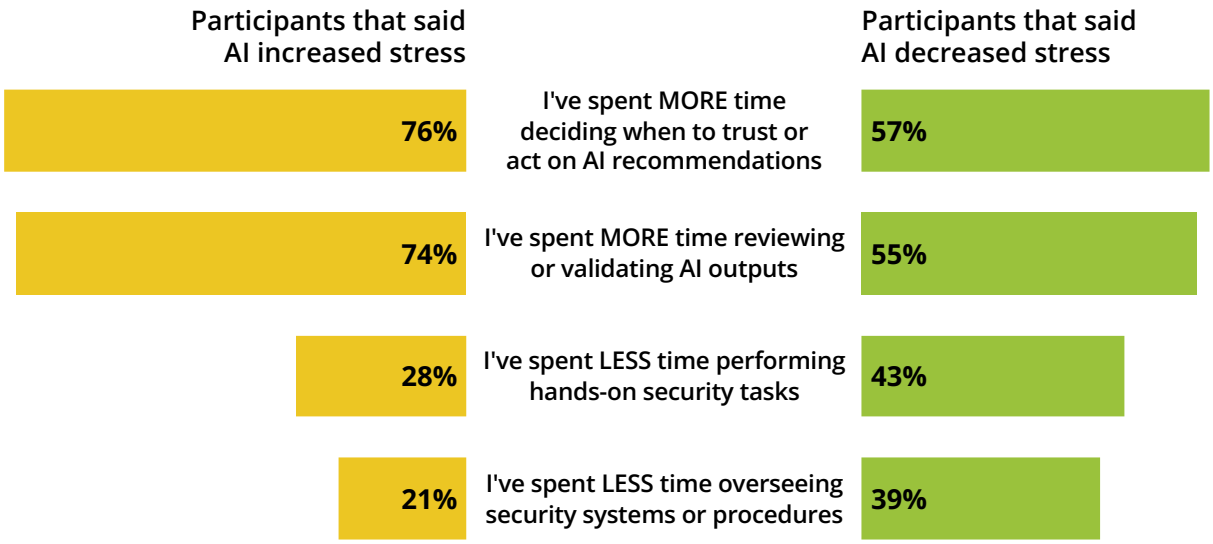
Is AI Usage Causing Work-Related Stress?



On further examination, differences in participants' stress levels over the past year are closely linked to how AI affected their workloads. Those who reported increased stress due to AI are significantly more likely than those with decreased stress to have spent more time deciding when to trust or act on AI recommendations (76% versus 57%) and reviewing or validating AI outputs (74% versus 57%).

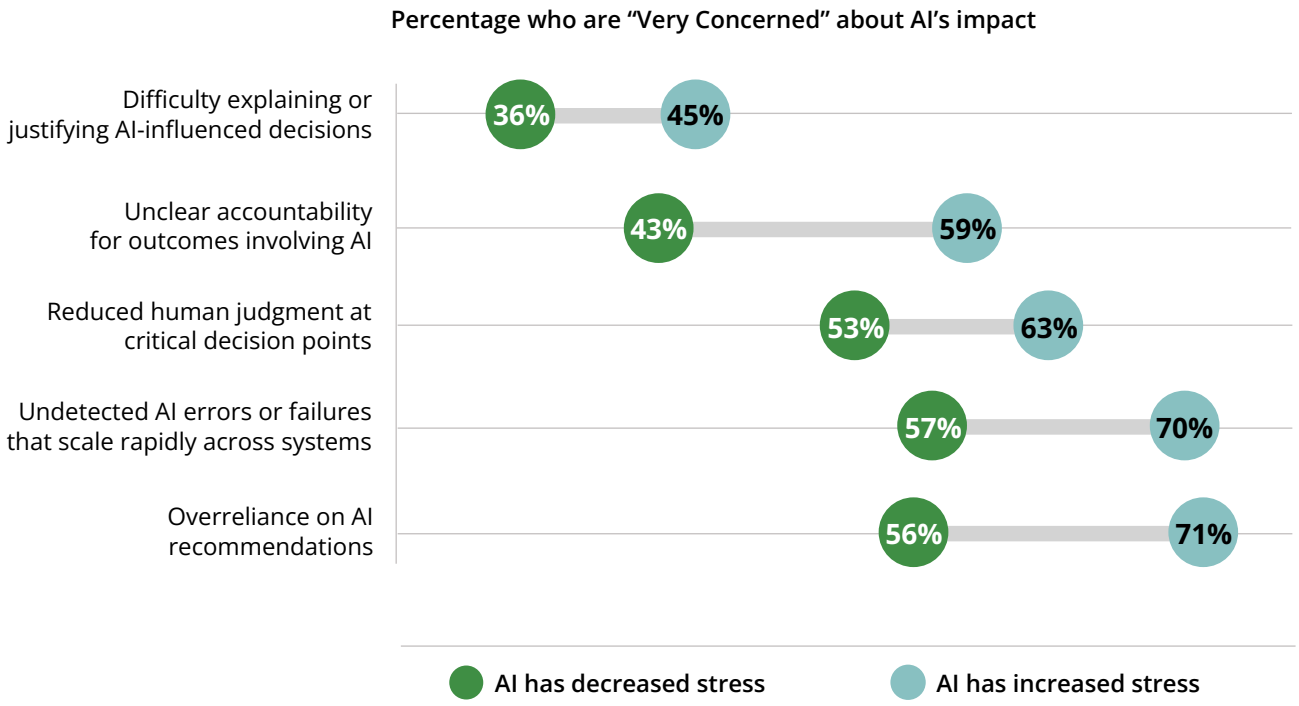
In contrast, participants who reported decreased stress because of AI are significantly more likely than those with increased stress to say AI has **reduced** the time they spend working on those same tasks and more.

Link Between Time Spent on Security Tasks and Work-Related Stress



This stress divide is also reflected in participants' concern about the potential impacts of more autonomous or self-directed AI systems use in security operations. Those who experienced increased work-related stress due to AI were significantly more likely to report high levels of concern about over-reliance on AI recommendations (71% versus 56%), undetected errors that could scale rapidly (70% versus 57%) and reduced human judgment at critical decision points (63% versus 53%). They were also more concerned about unclear accountability (59% versus 43%) and the difficulty of explaining AI-driven decisions (45% versus 36%).

Increased AI-Related Stress Tied to Greater Concern About its Impact in Cybersecurity Systems



There is a relationship between increased stress and the requirement to use unverified AI recommendations and actions. Participants who reported increased work-related stress due to AI were more likely to say they are often required to act on AI-generated outputs without fully understanding how those outputs were produced (34% versus 23% of those with decreased stress levels). In contrast, those with decreased (16%) or unchanged (18%) stress levels were more likely to say they have never faced this expectation, compared to those with increased stress levels (9%).

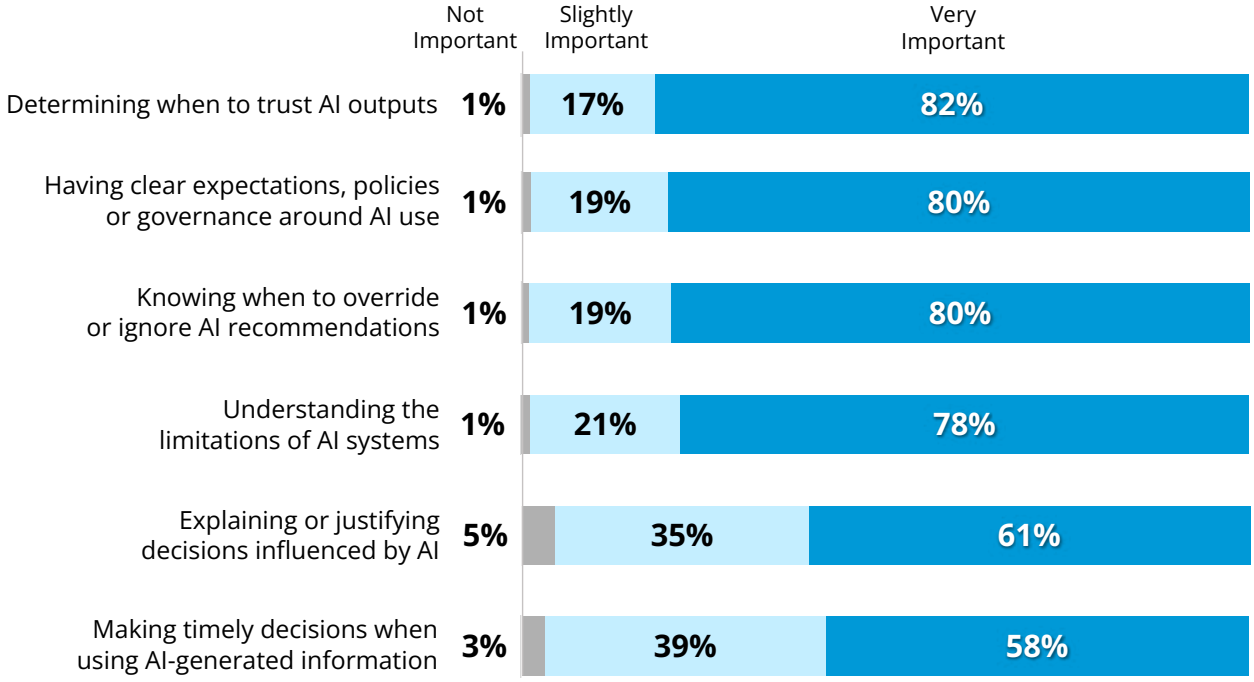
Perceptions of AI's long-term impact on careers also differ meaningfully by stress level. Participants who reported decreased stress were significantly more optimistic about AI creating new entry-level opportunities in cybersecurity (59% versus 46% of those with increased stress levels) and were significantly more likely to say AI makes them feel positive about their long-term career prospects
(59% versus 39% of those with increased stress levels and 37% of those with no change in stress levels).

The Importance of Effective AI Use

Given the many challenges, opportunities and inherent uncertainty that AI introduces within the cybersecurity profession, the effective use of AI depends **heavily** on clear practices and strong governance.

Most participants seem to recognize this and consider multiple factors important for effectively using AI in security work. Around 4 in 5 participants said that it's very important to determine when to trust AI outputs (82%), when to override or ignore AI recommendations (80%) and to have clear expectations, policies and governance frameworks around AI use (80%). Other critical must-haves include understanding the limitations of AI systems (78%), the ability to explain or justify AI-influenced decisions (61%) and making timely decisions when using AI-generated information (58%).

Rating the Importance of Factors for Effectively Using AI in Cybersecurity



Managing the Surge in AI-Identified Software Vulnerabilities

Participants provided valuable insight on how cybersecurity professionals can keep up with a faster and higher volume of AI-identified software vulnerabilities.

As one respondent noted:

> *"AI is turning vulnerability discovery from a slow, expert-bottlenecked process into a high-throughput pipeline. Our defenses need to match that throughput - not with more headcount, but with smarter workflows, better automation, and a team that's practiced at moving fast without breaking things further."*

That value of AI tools is illustrated by some of the adoption levels we are seeing. The **2025 ISC2 Cybersecurity Workforce Study** found that 28% of respondent organizations had already integrated AI tools into their security operations, 19% were actively testing them and another 22% were in the early evaluation phase.

Another respondent wrote:

> *"Cybersecurity teams must immediately shift to machine-speed defense: automate patching, adopt AI-driven vulnerability management, and strengthen real-time intelligence sharing to keep pace with the flood of AI-discovered software flaws. Traditional manual patch cycles are no longer sufficient—attackers are exploiting vulnerabilities within hours."*

In terms of where AI is expected to have the most impact on cybersecurity operations in the shortest amount of time, findings from the ISC2 Cybersecurity Workforce Study pointed towards network monitoring (40% of respondents), security operations and security testing (both at 30%), vulnerability management (29%), threat modeling and endpoint protection (both at 28%).

Actions and Recommendations

For many professionals, the challenge is not simply learning how to use AI tools, but keeping pace with a technology landscape that is evolving at an unprecedented rate. New AI models, platforms, features and best practices emerge almost continuously, creating pressure to remain up to date to stay productive, competitive and relevant. Beyond the quantitative findings above, participants' open-ended responses surfaced several strategies and technology decisions that will improve processes and better prepare cybersecurity teams for the safe and secure adoption and use of AI tools:

1. **Governance and guardrails:** Participants expressed a clear need for AI governance, with 80% viewing it as very important. Needs include defining processes, validation frameworks, audits and accountability at technical and leadership levels.

2. **Shift to AI-driven workflows:** Participants suggest embedding AI directly into security operations and pipelines.

3. **Faster, continuous remediation and patch management:** Participants emphasized moving toward real-time or continuous patching and improving vulnerability management processes to keep up with volume.

4. **Trust but verify (with humans):** Participants reported many concerns about false positives, hallucinations, and accountability that call for more human oversight, cross-validation and evidence-backed decision-making. Four in 10 respondents raised concerns over inadequate accountability regarding AI decision-making.

5. **Ensure AI operations don't negatively impact people:** A third (32%) of participants highlighted the relationship between unfettered AI use and an increase in stress and workload. As organizations continue to integrate AI into everyday business operations, understanding the relationship between AI adoption and employee wellbeing is increasingly important.

6. **Focus on skills development:** There were frequent calls for education in AI tools, underlying models, prompt engineering and broader cybersecurity fundamentals to keep pace with evolving threats.

As AI continues to evolve, employers and cybersecurity professionals at every career stage will need to adapt, develop new competencies and embrace a profession that is being reshaped, not replaced, by intelligent technologies.

About ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 270,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, the **Center for Cyber Safety and Education**, helps create more access to cyber careers and educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at **ISC2.org**. Connect with us on **X**, **Facebook** and **LinkedIn**.

ISC2™

ISC2.org

09/2026