REALITY CHECK:

Is AI Living Up to Its Cybersecurity Promises?

A Swimlane study conducted by Sapio Research

Table of Contents

Executive Summary

The rapid adoption of AI technologies, including generative AI (GenAI) and large language models (LLMs), has brought transformative changes to the cybersecurity sector. This shift has significantly enhanced productivity and efficiency for many organizations, prompting increased financial investment in AI-enhanced cybersecurity solutions.

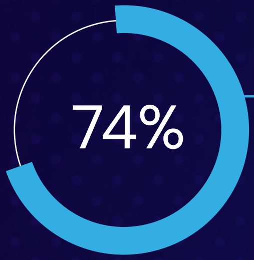
As AI becomes more integral to organizational operations, it also raises important discussions about the responsible use of these tools, including challenges related to data security, privacy, accountability, and the pervasive AI hype that can lead to fatigue.

To further explore these dynamics, Swimlane surveyed 500 cybersecurity decision-makers in the US and UK. The survey aimed to illuminate the growing need for a balanced approach to AI adoption, one that addresses both the opportunities and risks associated with this technology.

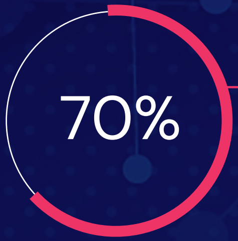
As AI becomes more integral to organizational operations, it also raises important discussions about the responsible use of these tools...

Key Findings

Is AI Making It Impossible to Balance Innovation and Confidentiality?

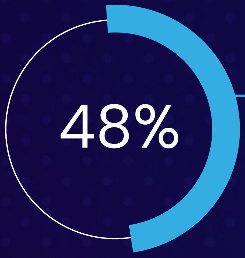


74% of those surveyed said they were aware of individuals at their organization inputting sensitive data into a public Large Language Model (LLM).

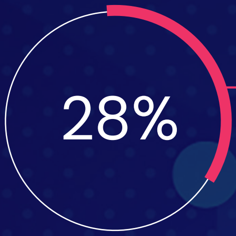


70% of organizations have specific protocols in place when it comes to what data is shared in a public Large Language Model (LLM).

Who Should Govern AI?

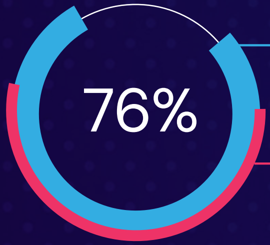


Almost half (**46%**) of respondents believe the company that developed the AI should be held primarily responsible for the consequences when AI systems cause harm.



Only **28%** of respondents believe the government should bear the primary responsibility for setting and enforcing guidelines.

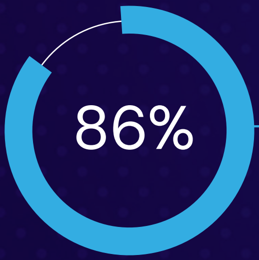
AI Hype or Growth Engine?



76% of respondents believe the current market is saturated with AI hype.

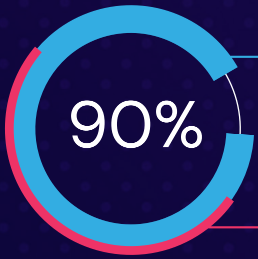
55% of respondents say they are starting to feel fatigued by the constant focus of AI, while **31%** disagree.

Are AI Skills Essential to the Cyber Workforce?



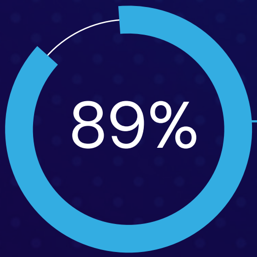
86% said experience with AI and ML tech is influencing hiring decisions to a great extent/some extent.

Will AI Adoption Fuel Efficiency Gains and Increased Budgets?



90% of organizations anticipate their overall cybersecurity budget will increase in 2025.

A third (**33%**) of organizations have more than **30%** of their current cybersecurity budget allocated to AI-powered or AI-enhanced solutions.

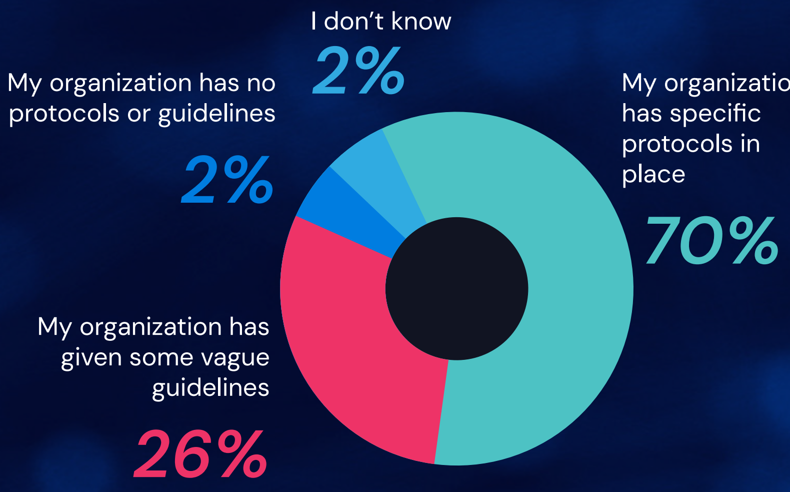


89% of organizations report that the use of GenAI and LLMs improved productivity and efficiency for their cybersecurity teams.

Is AI Making It Impossible to Balance Innovation and Confidentiality?

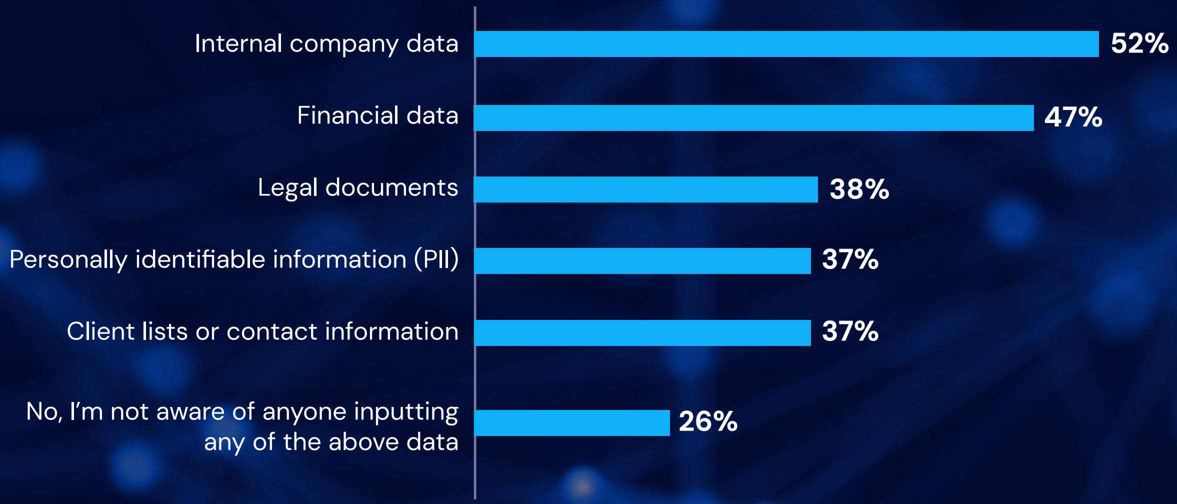
In the initial rush to embrace GenAI, companies implemented tools without fully considering the risks. Nearly two years after its rise, protocols exist but often fail to stop dangerous behavior. While **70%** of organizations have rules for sharing data with LLMs, **74%** admit to cases where sensitive information was still entered, showing a clear gap between policy and reality.

Does your organization have specific protocols in place when it comes to what data is shared in a public Large Language Model (LLM)?



This discrepancy raises questions about the effectiveness of these policies and whether they are being communicated, enforced or understood adequately by employees. The gap suggests that while organizations recognize the risks associated with data exposure in public AI models, there is still a significant challenge in ensuring that these policies translate into secure, everyday practices. As LLMs become more integrated into workflows, the need for robust, yet enforceable, data governance strategies becomes even more critical to balancing the benefits of AI with the risks it poses to data security.

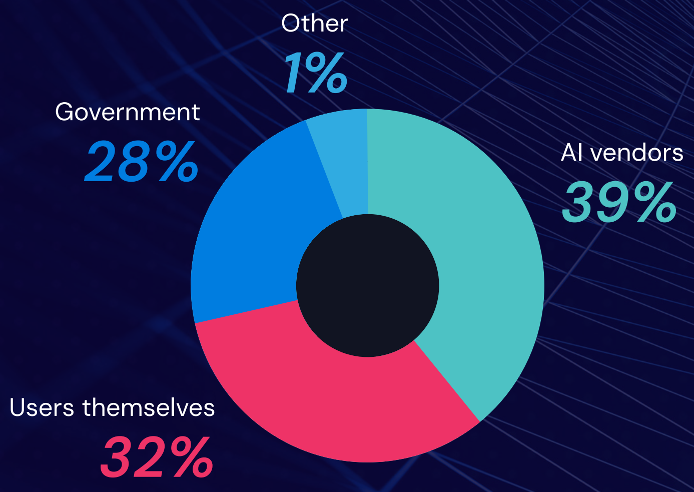
Are you aware of anyone at your organization that has ever input any of the following types of data into a public Large Language Model (LLM)?



Who Should Govern AI?

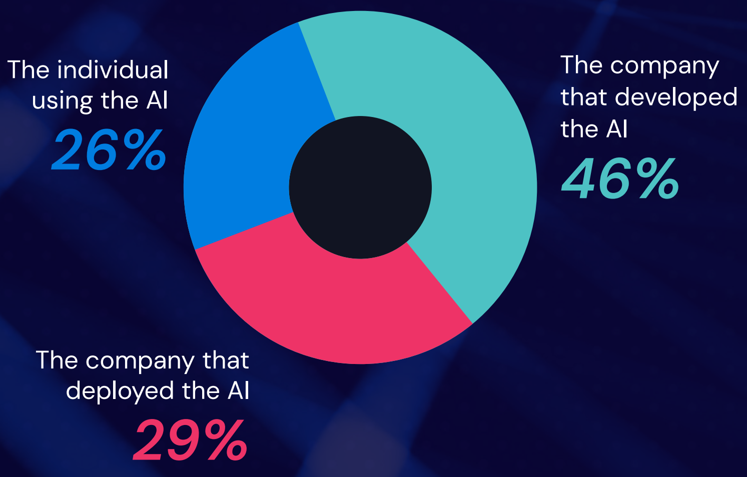
When it comes to ensuring responsible AI use, who do you believe should bear the primary responsibility for setting and enforcing guidelines?

As the hype around AI in cybersecurity collides with growing concerns over its potential risks, the question of regulation looms large. In recent months, various states and countries have introduced or proposed legislation aimed at governing the use of AI, from setting standards for transparency and accountability, to mandating risk assessments and audits. Yet, despite these ongoing calls for regulation, only **28%** of respondents believe that the government should bear the primary responsibility for setting and enforcing guidelines around AI use.



Instead, 39% believe that responsibility should fall squarely on the shoulders of AI vendors themselves. This might sound like the fox running the hen house, and while this divergence suggests there is a clear recognition of the need for oversight, many in the industry remain skeptical about the effectiveness of government intervention and look toward those closest to the technology—its creators and vendors—to take the lead in ensuring its safe and ethical deployment.

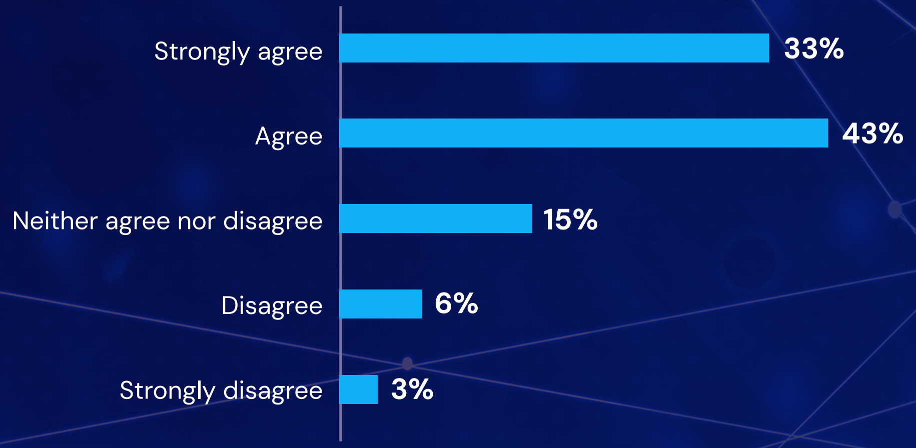
When AI systems cause harm, who do you believe should be held primarily responsible for the consequences?



When it comes to accountability for the harm caused by AI systems, opinions are divided. Nearly half (**46%**) of respondents believe that the companies developing these AI systems should be held responsible for any resulting damage. In contrast, **26%** think the responsibility should lie with the individual using the AI, while **29%** believe it should fall on the company that deployed the AI. This array of perspectives highlights the complexity of assigning accountability in the rapidly evolving AI landscape and underscores the need for clear and effective frameworks to address potential harms from AI technologies.

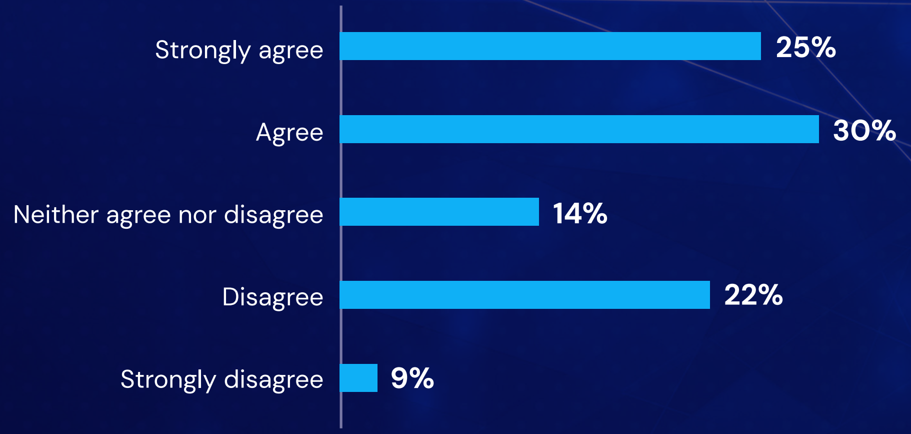
AI Hype or Growth Engine?

To what extent do you agree or disagree with the following statements? While AI tools show promise in addressing cybersecurity challenges, the current market is saturated with hype, making it more time-consuming to identify truly effective solutions.



In today's market, the saturation of AI hype is creating significant growing pains for organizations. A staggering **76%** of respondents believe the current landscape is overwhelmed with exaggerated claims of AI capabilities, making it increasingly difficult to discern which solutions are genuinely effective.

To what extent do you agree or disagree with the following statements? I'm starting to feel fatigued by the constant focus on AI in the media and everyday conversations



This overload of AI-centric messaging is taking its toll, with 55% of respondents expressing fatigue from the constant media buzz and everyday conversations surrounding AI, while **31%** remain less affected. The tendency to label every product as AI-powered, regardless of its true utility, contributes to the noise, frustrating teams that are already stretched thin.

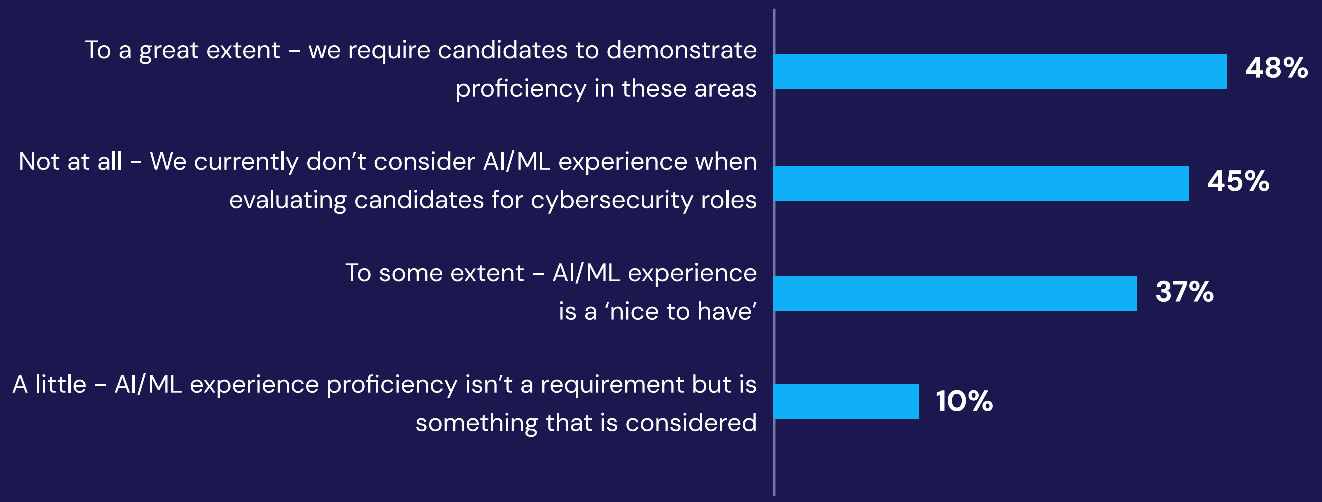
Despite the persistent hype machine, AI remains a critical tool at the epicenter of security operations. Its ability to enhance threat detection, automate responses, and streamline operations makes it an invaluable asset in the ongoing battle against cyber threats. As adversaries increasingly leverage AI to accelerate and sophisticate their attacks, the only way to stay ahead is to fight AI with AI. While the market may be cluttered with AI claims, the technology's strategic value in fortifying cybersecurity defenses cannot be overlooked.

Are AI Skills Essential to the Cyber Workforce?

Amid widespread concerns about AI potentially displacing jobs, a new narrative is emerging: one of opportunity and growth. With **86%** of organizations reporting that experience with AI and machine learning (ML) technologies significantly influences hiring decisions, it's clear that AI expertise is increasingly becoming a sought-after skill in the cybersecurity sector.

Rather than eliminating jobs, AI is reshaping the landscape, opening new doors for professionals equipped with these skills. As threats evolve, so does the demand for experts who can harness AI to predict, detect and mitigate these risks. For those willing to adapt and learn, AI represents a powerful tool—not a threat.

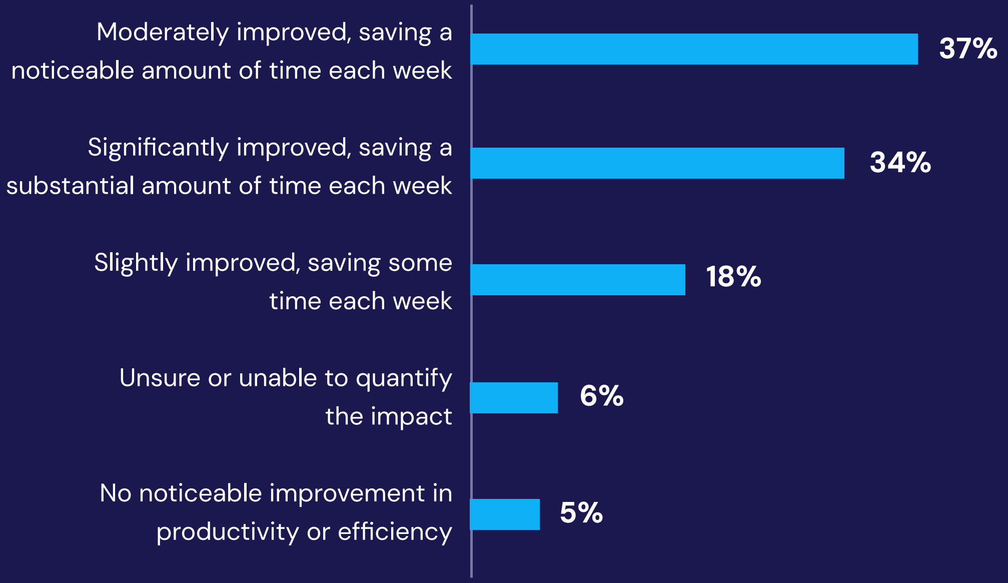
To what extent is experience with artificial intelligence (AI) and machine learning (ML) technologies influencing your hiring decisions for cybersecurity positions?



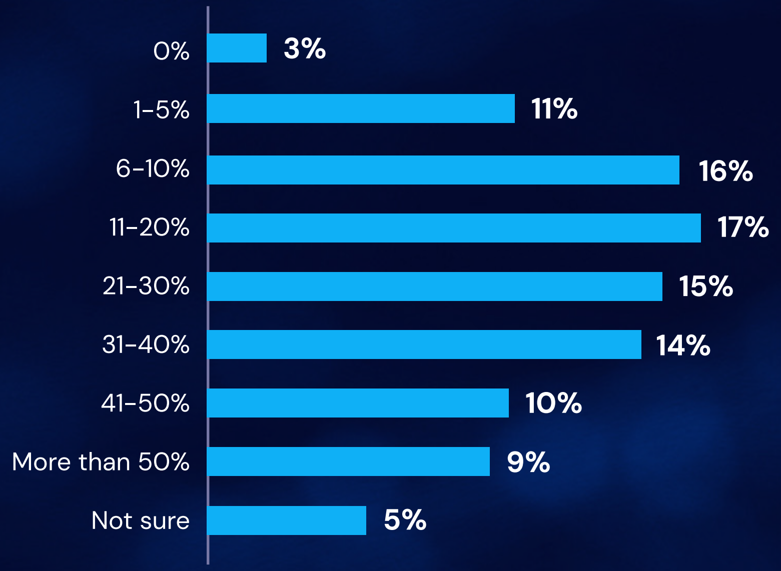
Will AI Adoption Fuel Efficiency Gains and Increased Budgets?

GenAI and LLMs have initiated a paradigm shift in the cybersecurity landscape, fundamentally transforming how organizations defend against the complex and persistent threats they face. An overwhelming majority of organizations (**89%**) report that the use of GenAI and LLMs has improved productivity and efficiency for their cybersecurity teams, resulting in significant time savings each week and ultimately improving overall security posture.

To what extent has the use of generative AI and LLMs improved productivity and efficiency for your cybersecurity team, resulting in significant time savings each week and ultimately improving overall security posture?



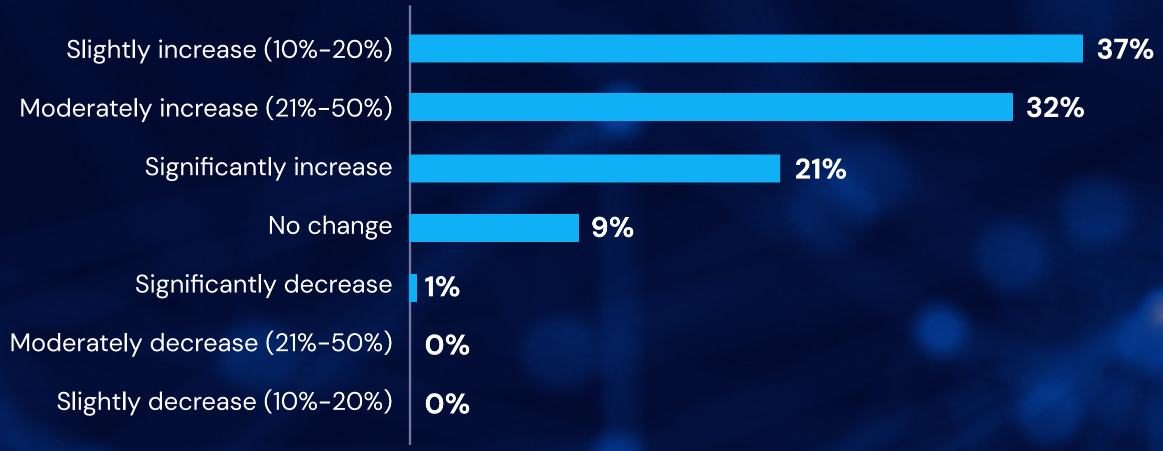
What percentage of your organization’s current cybersecurity budget is allocated to AI-powered or AI-enhanced solutions?



This surge in AI-driven performance is reflected in the financial commitment organizations are making toward these technologies. A third (**33%**) of organizations now allocate more than **30%** of their cybersecurity budgets to AI-powered or AI-enhanced solutions—a clear indication of a turning point in cybersecurity investments.

Looking ahead to 2025, do you anticipate your organization’s overall cybersecurity budget to?

In fact, 90% of organizations anticipate their overall cybersecurity budgets will increase in 2025, underscoring a broader recognition that increased spending on AI and other advanced technologies is essential to staying ahead of the curve. As these technologies become integral to defending against cyberattacks, the strategic shift towards AI is poised to reshape the future of cybersecurity spending.



The Risk, Rewards & Reality of AI

As AI continues to revolutionize cybersecurity, its influence extends far beyond the realm of digital defenses, touching on broader societal issues and challenges. A striking example is the concern that **74%** of respondents agree that AI-generated misleading information poses a significant risk to the U.S., particularly as we approach the 2024 elections. This highlights the dual-edged nature of AI technology—while it can enhance security and operational efficiency, it also brings significant risks that must be managed carefully.

Nevertheless, AI's overall impact on cybersecurity and beyond is profoundly positive. The technology is not merely a luxury but a necessity in a digital era where the volume, velocity, and sophistication of cyber threats are ever-evolving. By automating routine tasks and enhancing threat detection, AI is empowering human experts to focus on complex and strategic challenges, ultimately fortifying our defenses. Organizations that embrace AI are positioning themselves at the forefront of innovation, turning potential vulnerabilities into opportunities for stronger, more resilient security postures. As organizations and societies navigate these challenges, embracing AI responsibly and strategically will be crucial not only for enhancing cybersecurity but also for safeguarding democratic processes and public trust.

As AI continues to revolutionize cybersecurity, its influence extends far beyond the realm of digital defenses, touching on broader societal issues and challenges.

SWIMLANE

Methodology

The survey was conducted among 500 cybersecurity decision-makers at enterprise companies with at least 1,000 employees in the United States and United Kingdom. The interviews were conducted online by Sapio Research and under the guidance of Swimlane, Inc. in August 2024 using an email invitation and an online survey.

About Swimlane

Swimlane delivers automation for the entire security organization. Swimlane Turbine is the AI-enhanced, low-code security automation platform that unifies security teams, tools, and telemetry in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and ensuring overall security effectiveness.

About Sapio Research

Sapio's passion is giving clients confidence in their decisions, creativity, or storylines—helping them look good and be more productive. We do this by collecting and synthesising insight from qualitative, quantitative, or secondary research data sources. We focus on three key services: audience understanding, brand research, and thought leadership research.

Our high-quality tailored insights help improve lead generation and reputation, get you closer to your audience, and gain an edge against the competition. Through understanding, honest counsel, collaboration, and a swift approach we deliver projects you'll be proud of.

Best new agency finalist, Sapio is adept at opinion polling (we have access to 80 million people internationally), focus groups, face-to-face interviews, telephone interviews, online research, desk research and statistical modelling, to mention just a few techniques. We love B2B research and consultancy. Our business is based on partnership principles inspired by social enterprise.

CONTACT US
swimlane.com

GLOBAL HQ
999 18th St, Suite 2201N
Denver, CO 80202
1-844-SWIMLANE (1-844-794-6526)
info@swimlane.com

LONDON
4 Studley Court, Guildford Road,
Chobham GU24 8EB UK

MALAYSIA
Level 13A, Wisma Mont Kiara,
No. 1, Jalan Kiara, Mont Kiara,
50480 Kuala Lumpur,
Wilayah Persekutuan Kuala Lumpur

JAPAN
1-6-5, Kudan Minami, Chiyoda-ku,
Tokyo 102-0074

INDIA
1st Floor, Wing A, Purva Summit,
White Field Road, Kondapur, Hyderabad.