

Policy Backgrounder: AI and Cybersecurity

Rank Among Top 2024 Issues for CEOs

January 18, 2024

Trusted Insights for What's Ahead™:

Business leaders continue to focus on cybersecurity, labor shortages, and digital transformation as key priorities for 2024, underscoring the need for secure adoption of technology, clarity around guardrails for the use of artificial intelligence (AI), and upskilling of workers to fill roles for which there is great demand.

- In [The Conference Board's C-Suite Outlook for 2024](#), both global and US CEOs ranked the potential for increased cyberattacks as the #2 geopolitical risk; businesses are also focused on addressing labor shortages through technology adoption and investing in workers' capabilities.
- AI-enabled cyberattacks are expected to increase the sophistication and number of attacks, raising the urgency for organizations to bolster cyberdefenses by leveraging AI technology to identify and resolve vulnerabilities.
- While 90% of organizations are not prepared for a cyberattack, just 9% of CEOs cite cybersecurity as a critical investment choice for long-term growth.
- While nearly all CEOs expect AI adoption to enhance their firm's productivity, nearly half report that their organizations are not doing a good job identifying the business case for how AI should be used, while 94% believe that AI adoption will require new skills and training for their workers.

Cybersecurity is #2 Geopolitical Risk for Global CEOs

Both globally and in the US, CEOs rank the potential for an increase in cyberattacks as the #2 geopolitical risk for their business operations in 2024, according to The Conference Board's recently released C-Suite Outlook for 2024, [Leading for Tomorrow: Winning Through Change and Disruption](#). Among all other global C-suite participants, cyberattacks were the top geopolitical risk. The survey also reveals that while fewer than half of CEOs globally say their organizations are prepared to handle a cybersecurity crisis, just 9% of CEOs cite cybersecurity as a critical investment for long-term growth (14% in Europe).

Maintaining strong cybersecurity remains a fundamental challenge, and AI has only added to that challenge. The threat landscape has expanded as nation states and transnational organizations have developed ways to attack US organizations and infrastructure. Risks of cybersecurity attacks are largely borne by small- and medium-sized business, state and local governments, and individuals; for them, resources and expertise for cybersecurity are minimal. These challenges are amplified by [cyber labor shortages](#) in the US of 500,000 – a gap that grew over 2023 despite the growing threat.

As cyber threats have expanded, companies have made larger investments to secure their organizations. On average a company's cybersecurity cost is 5% to 8% of its technology [spending](#). In addition, the cost of cybersecurity insurance is rising as the market [continues to mature](#). Every day, there are 4,000 [new attacks](#), and bad actors send these attacks to many organizations to ensure they are propagated widely. Yet 90% of organizations report they are [not prepared](#) for an attack on their infrastructure.

New regulations, including the Security and Exchange Commission's [cyber incident reporting rules](#) for public companies, [require](#) firms to disclose material breaches within four days of discovery, in addition to

bolstering their governance and risk management of cyber threats. However, few companies today have the internal infrastructure [ready](#) to identify and respond to attacks within the required period. In the face of rapid technological advances, companies should build roadmaps to integrate and modernize cybersecurity systems to make them secure by design.

To help address the nation's cyber vulnerabilities, the Administration published its [National Cybersecurity Strategy](#) in March 2023. The plan aims to both realign incentives to encourage long-term investments and to shift the responsibility of cyberdefense to those who can most bear it, including the federal government and large digital service providers. Cooperation is at the Strategy's core, as the private sector owns a significant portion of the infrastructure necessary for cybersecurity. A significant initiative under the plan was the release of the [National Cyber Workforce and Education Strategy](#), outlining a comprehensive approach to address the immediate and longer-term need to build a robust cyber workforce. Raising broader awareness of the need for workers in addition to enrolling more students and workers in computer science and workforce development programs are opportunities for greater public-private collaboration for strong cybersecurity.

These priorities and concerns of CEOs accord with CED's Solutions Briefs related to securing the nation's cyberdefenses, [Securing Cyberspace in an Era of Evolving Threats](#) and [Securing Critical Infrastructure: Building Resilience](#).

AI to Shift Nature of Cybersecurity

Rapid advances in AI challenge business leaders and policymakers to accelerate planning to leverage the opportunities AI presents while mitigating risks. Greater uses for AI will continue expanding the threat landscape, enhancing the number and sophistication of adversarial cyberattacks. Today's leading cyberattack methods — email and phishing — will become an even greater weakness as AI capacity accelerates. Bad actors are also expected to leverage AI for new malicious attacks, for example building new types of malware or crafting effective, fabricated deepfake images and videos.

To combat AI-enabled cyberattacks, companies must make use of AI tools that are capable of analyzing large quantities of data and identifying vulnerabilities. The large quantities of data involved in responding to cybersecurity attacks of the future cannot be processed by humans alone. Instead, the economy needs more workers skilled in AI who can set up these systems for responding to attacks, rather than continually expanding the number of dedicated cybersecurity professionals tasked with manual detection and remediation. The [2024 C-Suite Outlook](#) survey highlights this dynamic in organizations' planning. Labor shortages and rapidly advancing AI each rank among CEOs' top external challenges, while accelerating the pace of digital transformation, increasing automation, and upskilling talent are all top management priorities for 2024. However, while close to 90% of CEOs expect AI to enhance their firm's productivity, nearly half report that their organizations are not doing a good job identifying the business case for how AI should be used, and 94% believe that AI adoption will require new skills and training for their workers.

While the US lags the EU and China in establishing a comprehensive AI regulatory framework, [surveys](#) suggest that more than three-fourths of Americans support government regulation to mitigate risks, including discrimination or biased practices, the spread of misinformation, and the impact on jobs and inequality. Progress on AI regulation is occurring slowly, with Congress [convening hearings](#) aimed at deepening policymakers' understanding of AI and its risks, and the Administration and Congress developing principles and [frameworks](#).

Conclusion

Cybersecurity remains a top geopolitical risk to businesses in 2024, highlighting the need for continued focus from both business leaders and policymakers to bolster cyberdefense. As the capabilities of AI technologies grow, malicious actors will seek to leverage the technology to expand the sophistication and number of cyberattacks exponentially. This puts tremendous pressure on businesses, particularly with respect to consumer-facing platforms and those housing large amounts of data in the cloud.

The National Cybersecurity Strategy, which has been [lauded](#) by cyber experts, set in motion a comprehensive plan to address cybersecurity vulnerabilities — particularly related to infrastructure and the lack of a robust cyber workforce — as a key [bipartisan](#) national security issue. Efforts across federal departments have also accelerated in the past year. The [Department of Defense](#) issued its updated 2023 Cyber Strategy, while the [Department of Justice](#) announced it would establish a National Security Cyber Section within the National Security Division. However, deepened collaboration with the private sector will be key to achieving the goals of the overall National Cybersecurity Strategy.

Other solutions for companies may include developing roadmaps to modernize cybersecurity systems in addition to planning now for how companies will leverage AI tools. This may require companies to elevate technological expertise within their organizations, craft governance structures to manage AI risks, develop guidelines for vendors and platforms, and educate their employees while reassessing future job roles.

Further, regulatory uncertainty should not deter companies from taking immediate action to assess the potential role of AI in their organizations and helping to shape still-developing US regulatory policies. CEOs and their management teams seeking to use AI can commit to elevating technological expertise within their organizations. More broadly, both business leaders and policymakers must consider the larger challenge of how to structure guardrails around the use of AI that both allow innovation and at the same time protect both companies and the global economy from threats associated with the use of AI, including cybersecurity threats, privacy, deep fakes, untrustworthy data, and other risks.

About the Authors

[John Gardner](#) is the Vice President of Public Policy at the Committee for Economic Development, the public policy center of The Conference Board.

[Mitchell Barnes](#) is a Senior Economic Policy Analyst at the Committee for Economic Development, the public policy center of The Conference Board.

About The Conference Board

The Conference Board is the member-driven think tank that delivers Trusted Insights for What's Ahead™. Founded in 1916, we are a non-partisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States. www.ConferenceBoard.org

The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led organization delivers well-researched analysis and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today's pressing policy issues. Collectively, they represent 30+ industries and over 4 million employees. www.ced.org