Trellix

The Mind of the CISO: Decoding the GenAI Impact

Over 500 security executives share how AI is changing the CISO role and the cybersecurity landscape

Contents page

Executive Summary

A CISO's Perspective of GenAI:
The Strange Case of Dr. Jekyll and Mr. Hyde

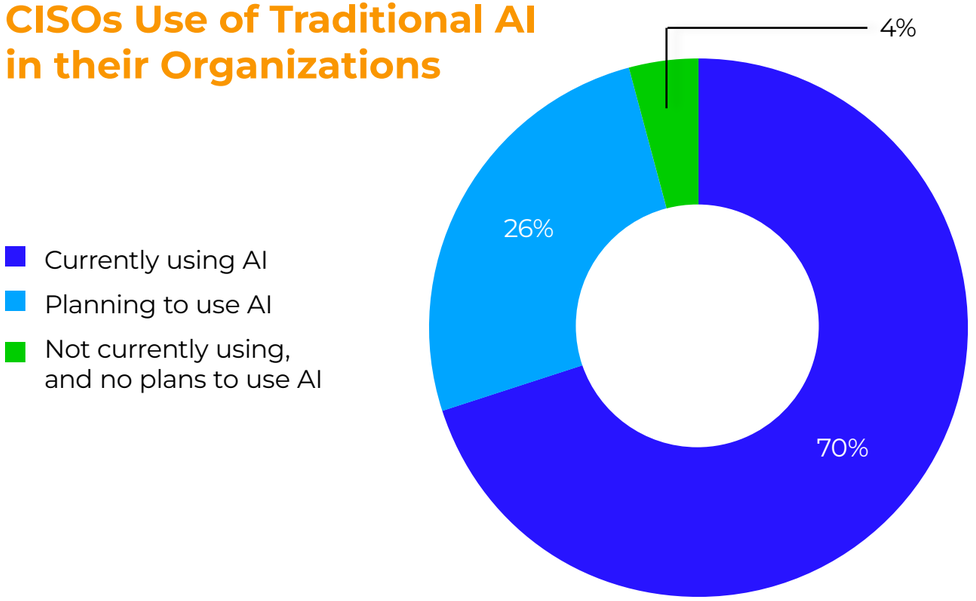
The role of the Chief Information Security Officer (CISO) is once again in the spotlight following high-profile cases like the Securities and Exchange Commission's (SEC's) fraud charge brought against SolarWinds CISO after the 2021 breach. The increased use of Artificial Intelligence (AI) further complicates this role as industries begin to realize the full potential of Generative AI (GenAI) and its impact on cybersecurity.

GenAI has rolled out at an immense speed, presenting a challenge for CISOs to secure critical data within their organizations. The democratization of GenAI means it can now be used at every professional and skill level, bringing with it a range of benefits as well as potential issues with both offensive and defensive capabilities in cybersecurity.

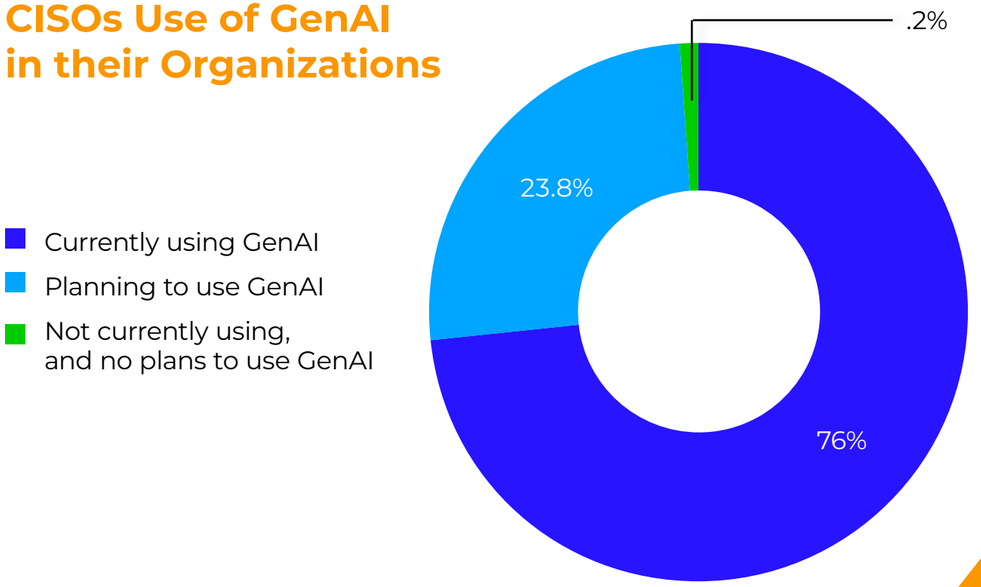
Trellix commissioned independent market research agency Vanson Bourne to conduct a research survey of 500 CISOs across North America to understand their perceived risks and benefits for using GenAI within security operations at their organizations. Respondents work across a range of industries, including finance, public sector, healthcare (public and private), manufacturing, energy, oil, gas, and utilities. The results clearly show CISOs are already feeling the impact of GenAI on their organization, team, and role.

76% of CISOs already use GenAI in their organizations, with most of the remaining 24% planning to. 70% currently use traditional AI, with 26% reporting they plan to do so in the next 12 months, with the most common applications being predictive analytics software and natural language processing (NLP) tools.

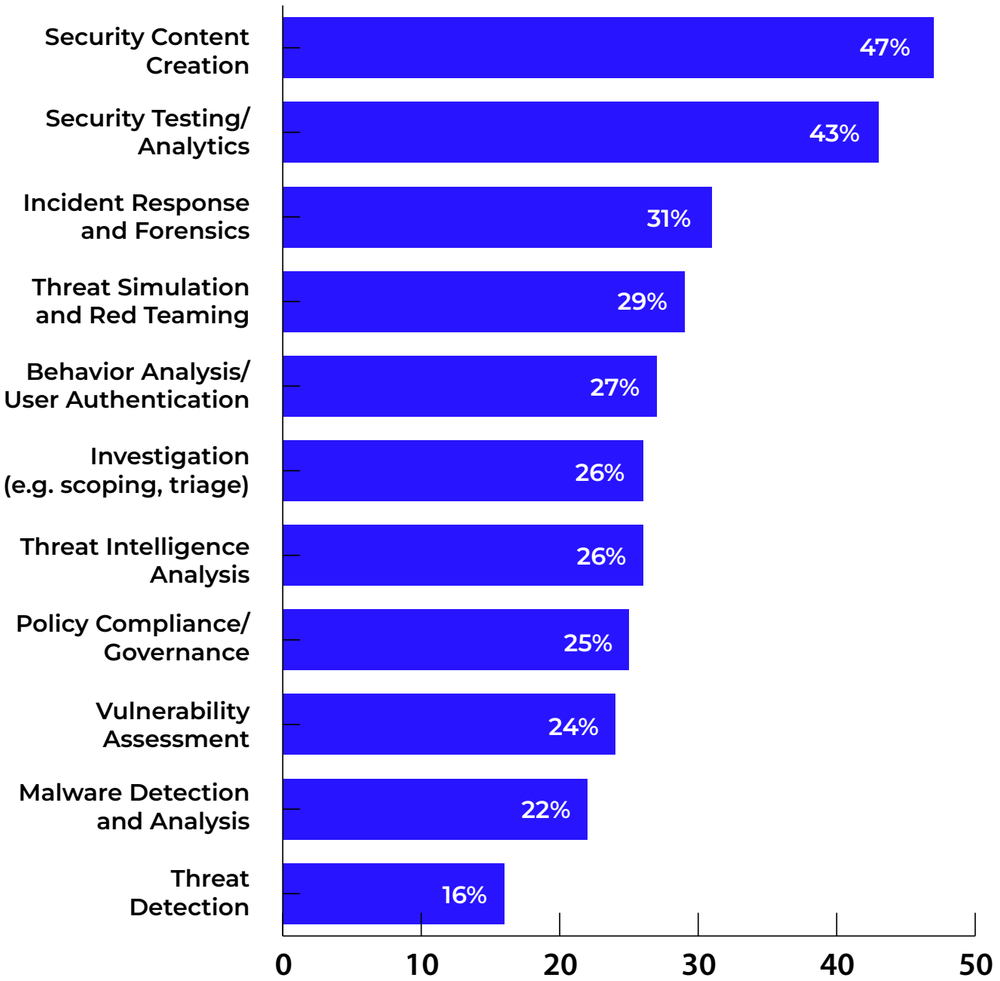
CISOs Use of Traditional AI in their Organizations



CISOs Use of GenAI in their Organizations



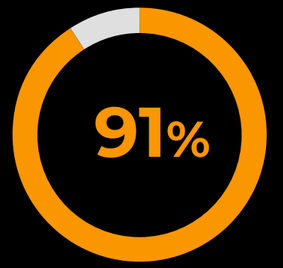
Processes/Technologies Enhanced/ Augmented by GenAI



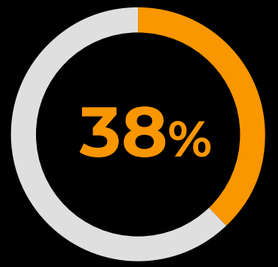
All (100%) respondents from organizations already using GenAI believe it is enhancing/ augmenting cybersecurity processes and/or technologies.

CISO's know GenAI has the power to revolutionize how organizations operate. All (100%) respondents from organizations already using GenAI believe it is enhancing/augmenting cybersecurity processes and/or technologies.

With this technology becoming such an essential part of daily functioning, it's clear the role of the CISO and the future of cybersecurity in the workplace is being reshaped. CISOs have recognized the benefits, with 91% expressing excitement over the prospects and opportunities GenAI and AI will bring to their organization. On average, CISOs believe GenAI has or could improve the productivity of their organization's workforce by 38%.



91% of CISOs expressed excitement over the prospects and opportunities GenAI and AI will bring to their organization.

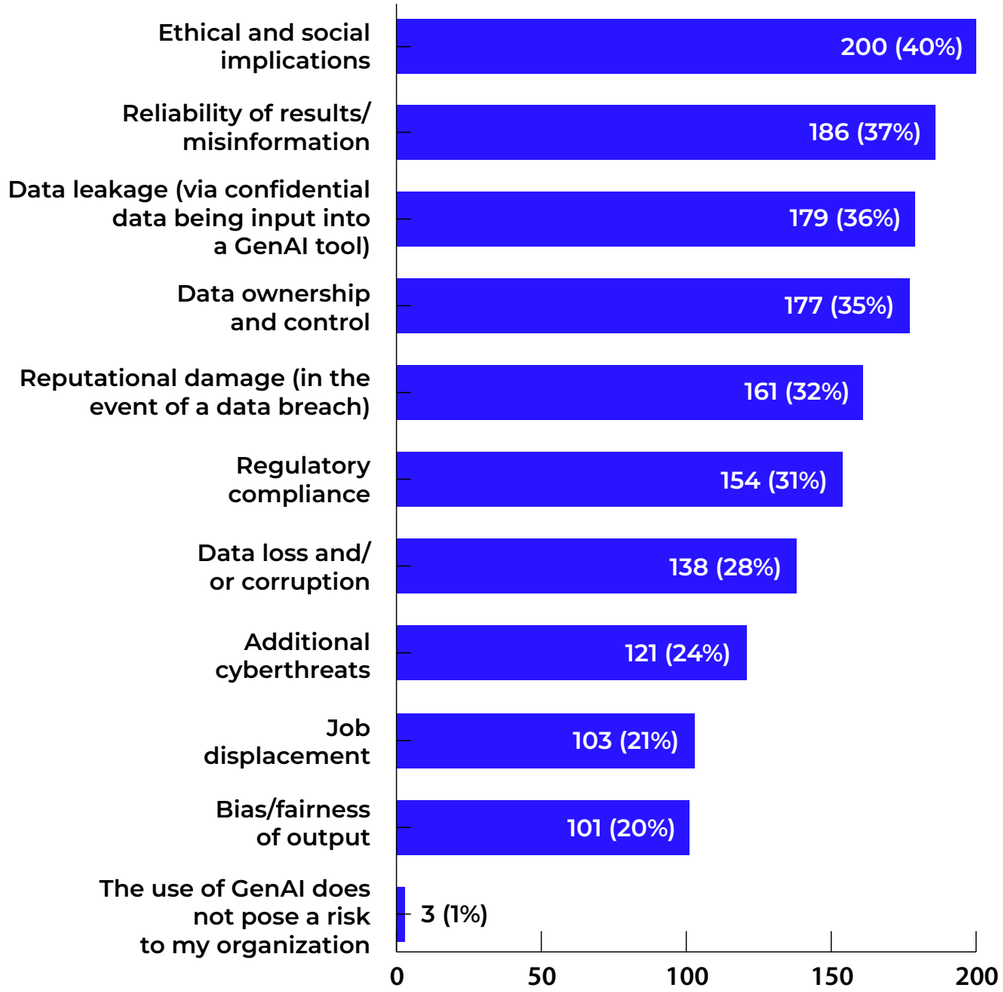


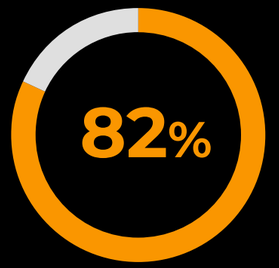
On average, CISOs believe GenAI has or could improve the productivity of their organization's workforce by **38%**

AI can offer significant advantages, but almost all CISOs surveyed (99.8%) believe there are multiple areas which require greater levels of regulation, particularly surrounding data privacy and protection and ethical use.

GenAI is a double-edged sword with the power to both enable and defend against serious cyber threats, and CISOs recognize the risks. While CISOs are leveraging GenAI and AI, almost all (99.8%) respondents are concerned about *cybercriminals' using GenAI* to

Risks CISOs foresee as a result of their organizations using GenAI (for CISOs already using or planning to use GenAI)





82% of CISOs reported an increase in the number of cyberattacks over the past six months

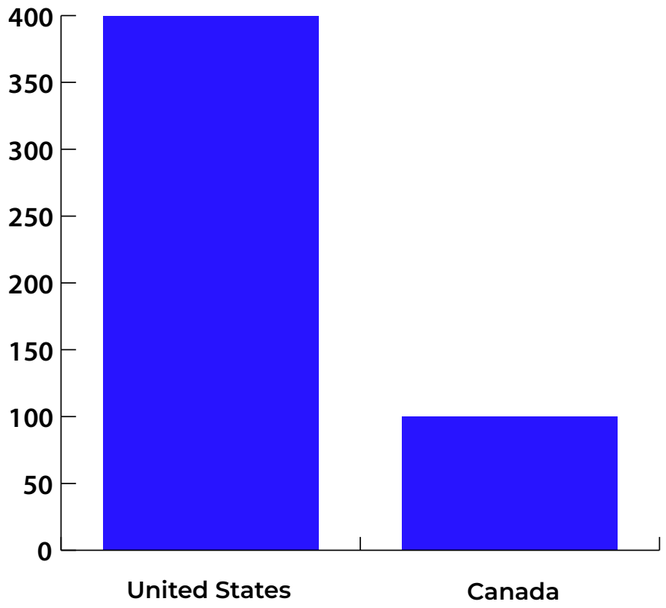
perform cyberattacks, with an increase in speed, frequency, and scale, especially since 82% of CISOs reported an increase in the number of cyberattacks over the past six months. The top three risks CISOs foresee from their own organizations using GenAI are the ethical & social implications, reliability of results/ misinformation, and data leakage.

With these changes, the next question is how the CISO's role will need to adapt to keep up with this environment. Keeping pace with AI and GenAI is vital, and almost all respondents said their organizations could be doing more.

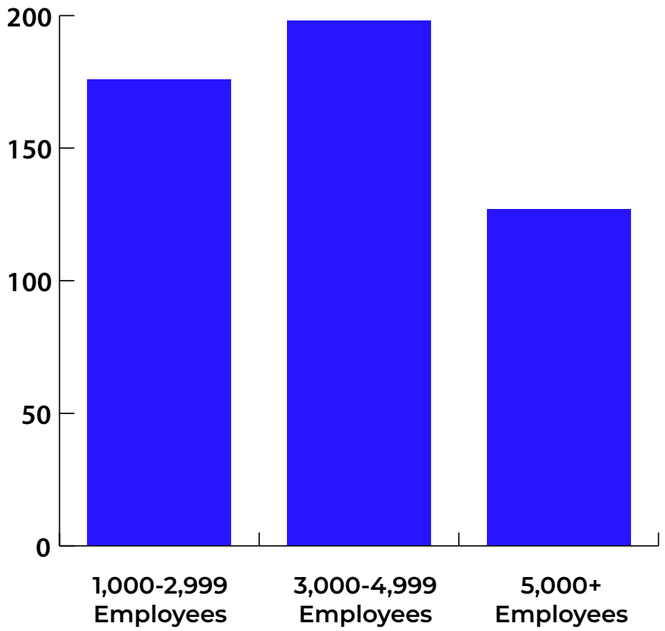
Respondent Profile

500 CISOs (or equivalent) were interviewed in March/April 2024, split in the following ways...

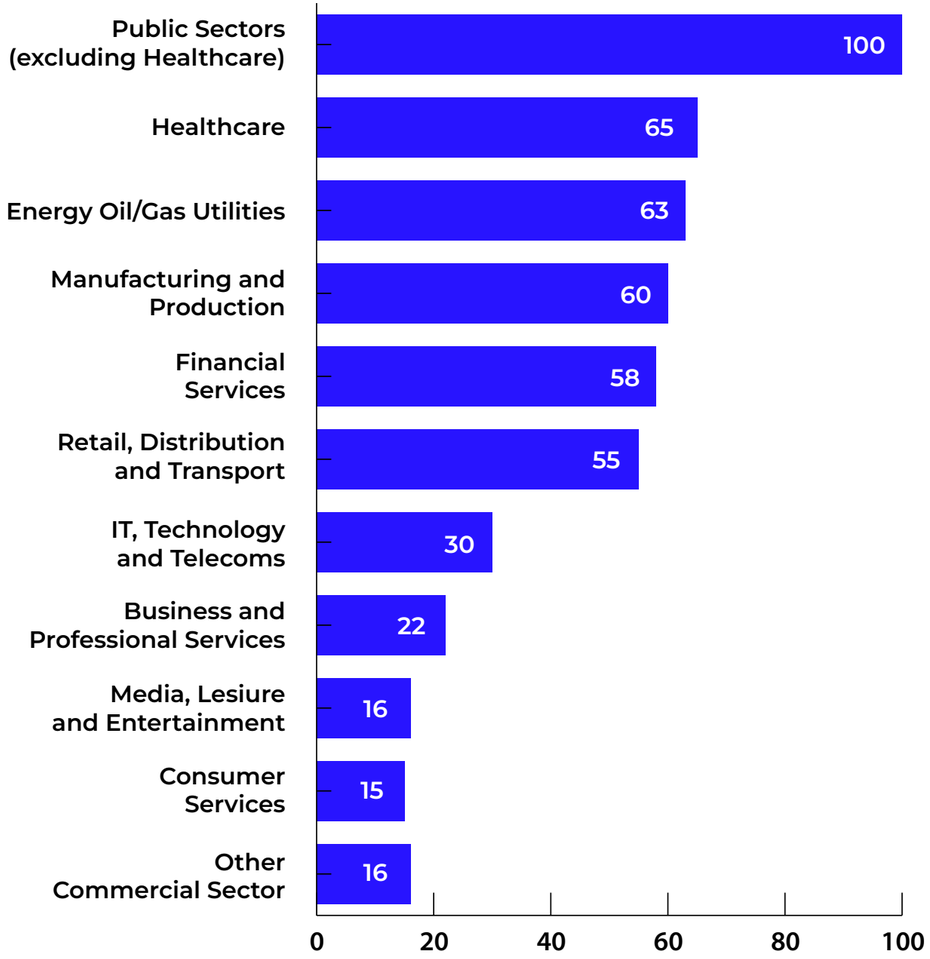
... by respondent country



... by organization size



... by organization sector



Key findings

- GenAI will have the power to revolutionize how the cybersecurity workforce operates. CISOs overwhelmingly say they understand the implications, and 100% believe the technology will enhance/augment cybersecurity processes and technologies.
- With the introduction of GenAI, the Trellix Advanced Research Center has seen an increase in cyberattacks over the last six months, and there is evidence of Russian criminal groups possibly using ChatGPT to survey and collect data from other cybercriminals to expand and further develop their operations. CISOs reported being most concerned about edge computing, malicious learning, prompt injection, AI-powered bots, and GenAI technologies being used in cyberattacks.
- The public sector is acutely vulnerable because it has been slower in adopting GenAI in daily operations, leaving it more open to attacks.
- The introduction of AI/GenAI in organizations has drastically increased day-to-day stress, with 68% of CISOs saying AI is increasing their day-to-day stress levels, 31% of them saying it has significantly increased. The majority of CISOs (92%) agree AI/GenAI has made them contemplate their future as a CISO.

82%

of organizations have experienced an increase in cyber attacks over the past 6 months

84%

believe GenAI could give their organization an advantage over cybercriminals

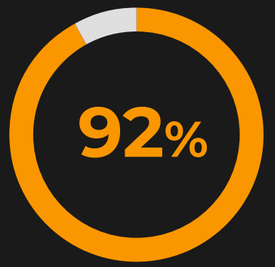
90%

of CISOs feel they are exposed to increased liability as a result of AI/GenAI

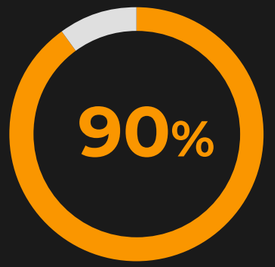
92%

of CISOs agree AI/GenAI has made them contemplate their future as a CISO

AI presents a double-edged sword; and in the wrong hands, it can pose significant security risks. Almost all **(99.8%)** respondents are concerned over cybercriminals using GenAI to perform cyberattacks, with an increase in speed (38%), frequency (37%) and scale (37%) of attacks the most prevalent concerns.



92% of CISOs say using GenAI without clear regulations would put their organization at risk, with nearly all (99.8%) agreeing greater levels of regulation are required in the next 6 months; particularly surrounding data privacy and protection (55%).

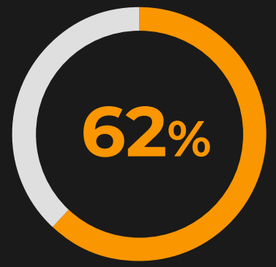


With cyberattacks on the rise, AI pressures mounting, and responsibilities growing, it's no surprise **90% of CISOs** are finding themselves under increased pressure.

Section one

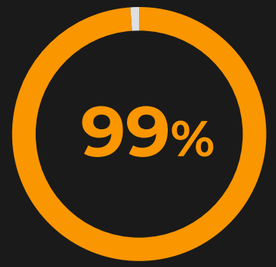
GenAI and Cybersecurity: The Risks and Benefits

GenAI has transformed the cybersecurity landscape, enabling cybercriminals to unleash attacks at an unprecedented scale. The barrier to entry for committing large-scale cyberattacks has been lowered due to *Large Language Models (LLMs) such as ChatGPT*, which are now free or commercially available to the public. These advancements enable nation-state and criminal actors to improve offensive tactics, essentially turning cybersecurity into an arms race where attackers can leverage cheap AI models to surpass conventional defense mechanisms. The use of ChatGPT can increase the sophistication of crude cyberattacks like phishing.



62% of CISOs don't have full confidence in their organization's workforce to successfully identify cyberattacks incorporating GenAI

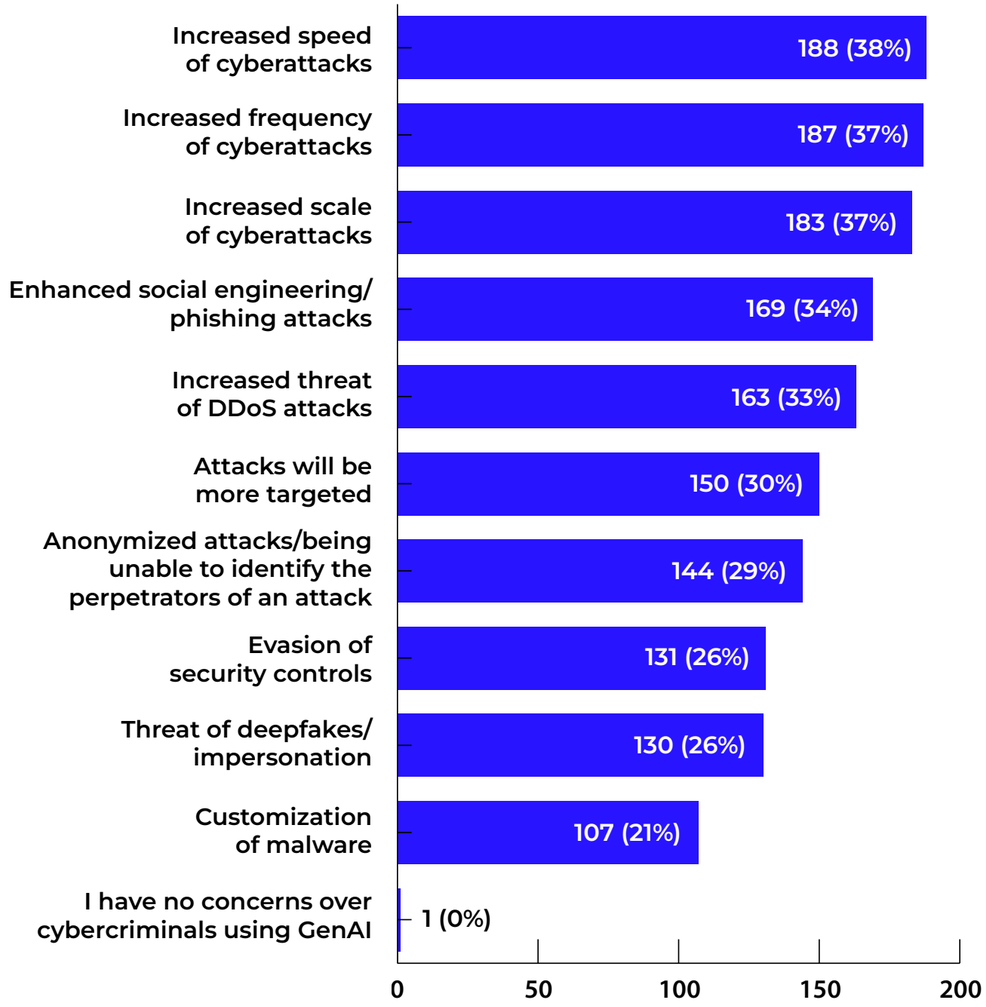
GenAI provides cybercriminals with increased capabilities to craft phishing attacks in multiple languages, with near-perfect grammar and syntax, making it harder for organizations to detect them. There have been active attempts by companies like OpenAI (the parent company of ChatGPT) to reduce these threats, with a direct focus on state-actors. The harder task is how to detect non-state cybercriminal actors, whose dispersed nature online makes them more difficult to track.



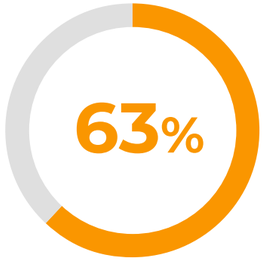
99% of CISOs reported experiencing a cyberattack in the last six months

CISOs are already noticing these threats and gaps within their organizations, with 62% of respondents agreeing they don't have full confidence in their organization's workforce to successfully identify cyberattacks incorporating GenAI. This is especially concerning, considering 99% of respondents reported experiencing a cyberattack in the last six months, with 82% experiencing an overall increase in cyberattacks. Primary concerns relate to the speed, frequency, and scale of cyberattacks GenAI will enable.

What concerns, if any, do you have over cybercriminals using GenAI to perform cyberattacks?



Concerns over security are also becoming more sector-dependent, particularly in the public sector and how CISOs see the threat of GenAI to data protection and vulnerability to attacks. The public sector has been the slowest of all surveyed to adopt AI practices. This may be due to budget constraints and legacy technology, which hasn't been updated since the introduction of commercial GenAI. The slow pace is particularly concerning when the data clearly shows the public sector (excluding healthcare) reported the highest increase in cyberattacks.



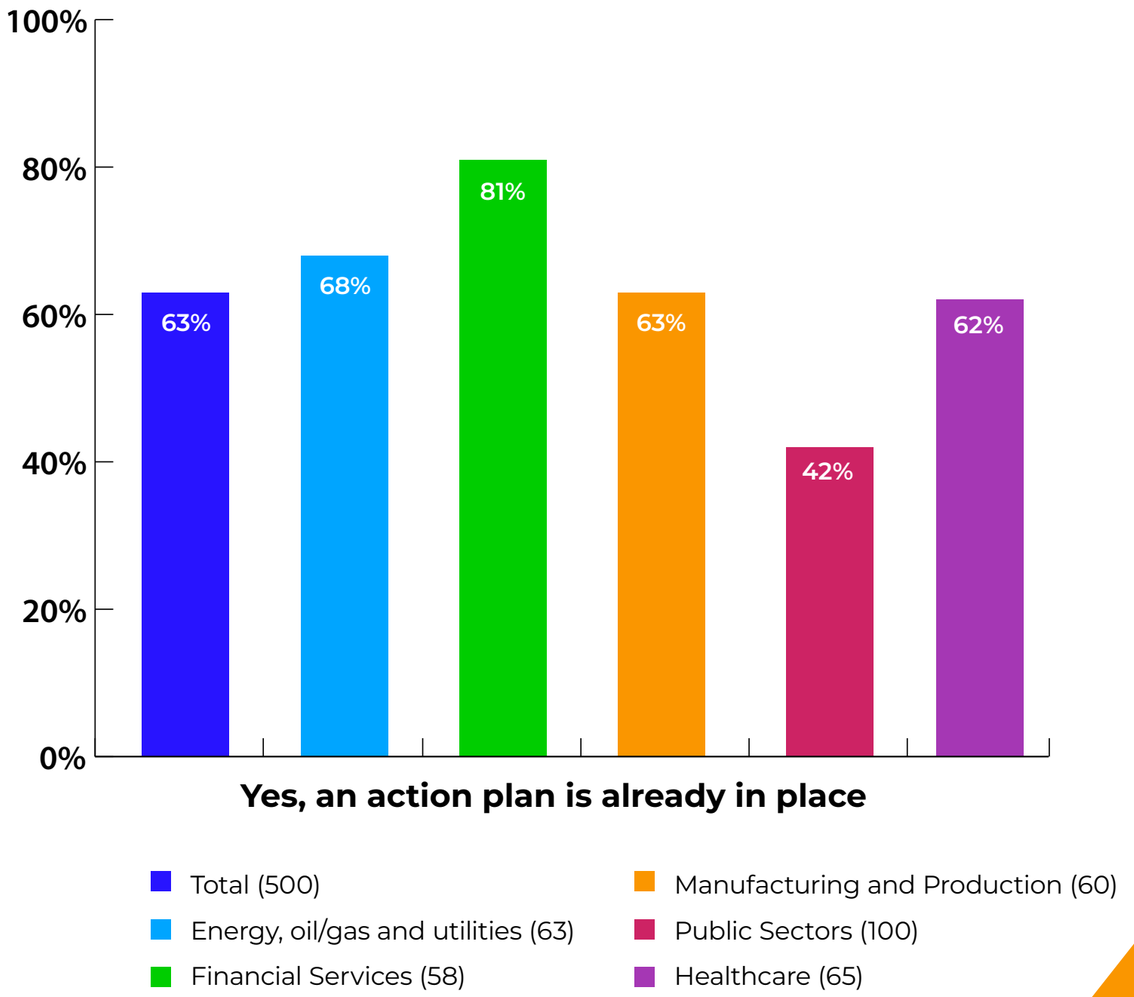
63% of CISOs said their organization currently has an action plan in place for training and guidance on AI tool use and threat detection for its employees

Top three key industries most likely to report an increase in cyberattacks

1	Public sectors (excluding healthcare) [100]	95%
2	Manufacturing and production [60]	87%
3	Financial services [58]	84%

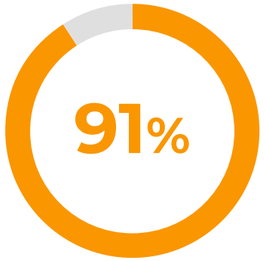
The public sector was also the lowest-reported industry by CISOs with an action plan in place for training and guidance on AI tool use and threat detection. 63% of overall respondents already have an action plan in place for AI training and guidance. These vulnerabilities are even more worrying when considering the sensitive data contained by the public sector and the threats critical infrastructure faces from adversaries, making the role of the CISO in this sector especially pertinent. The digitalization of essential functions leaves it uniquely exposed to attacks. The lack of readiness expressed by CISOs in the public sector shows a clear need for increased funding and an expanded workforce.

Currently have an action plan in place, split by key industries



Another area of concern is the prevalence of ransomware attacks, and the introduction of GenAI to the threat landscape has only heightened these risks. 93% of CISOs agreed ransomware incorporating AI is a significant risk to their organization. In the first half of 2023, ransomware attacks *increased globally* by 45% and impacted critical infrastructure, including hospitals, manufacturing, and food supplies. In the United States alone, an estimated $1.3 billion in ransom payments were made from U.S. organizations from mid-2022 to mid-2023. The Mind of the CISO research data shows the highest point of concern for healthcare sector respondents is data and privacy, with 62% of respondents listing it as their top concern. This is particularly worrying in a sector notoriously hit by ransomware attacks and acutely vulnerable to the threats posed by GenAI. However rampant these threats are, CISOs also believe AI can provide a line of defense against these attacks. 91% agreed AI can help protect their organizations from ransomware.

93% of CISOs agree ransomware incorporating AI is a significant risk

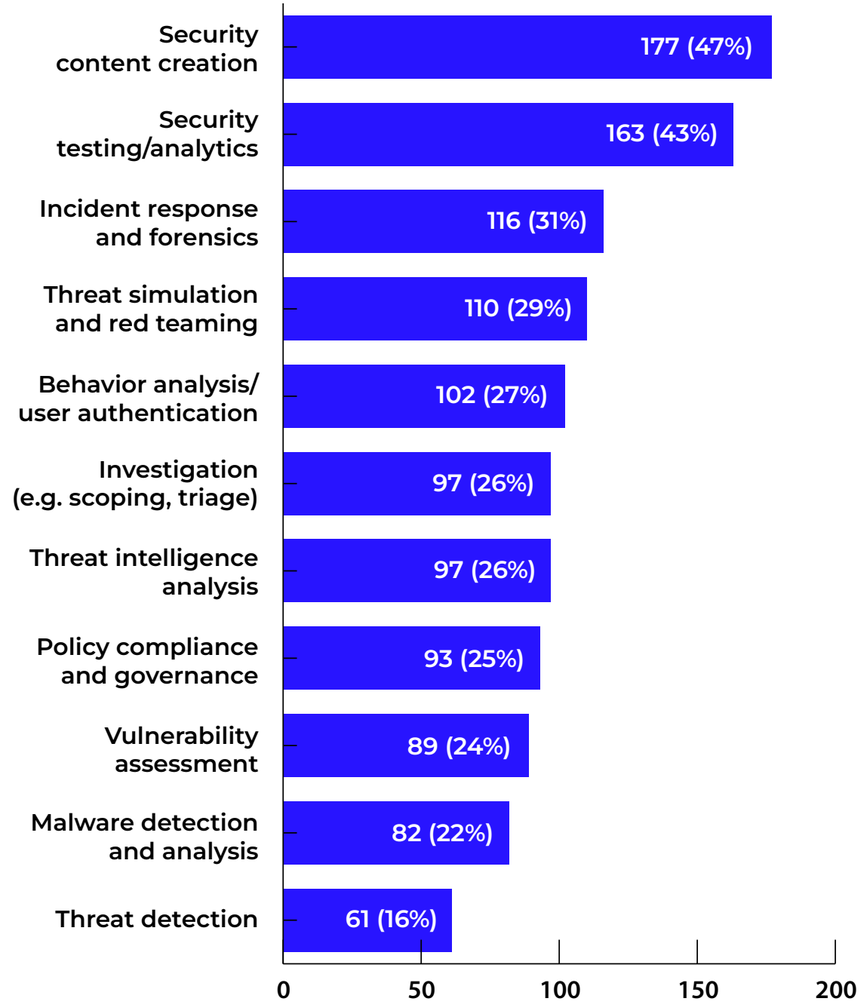


91% of CISOs agreed AI can help protect their organizations from ransomware

To combat the evolving strategies of cybercriminals, CISOs can harness AI technology to proactively defend against these threats. Almost half (47%) of respondents identified they are already using GenAI to enhance security content creation and another 43% are using it in security testing and analytics. Overall the survey data shows a promising pattern towards adopting AI and GenAI as a countermeasure in cybersecurity, with 84% of respondents agreeing it could actually help organizations gain an advantage over cybercriminals. The data clearly shows how AI and GenAI present a complex balance between risk and defense in cybersecurity, but CISOs are willing to lean in to gain a strategic edge in this shifting threat landscape. Section three of this report outlines additional perceived or realized benefits of this technology.

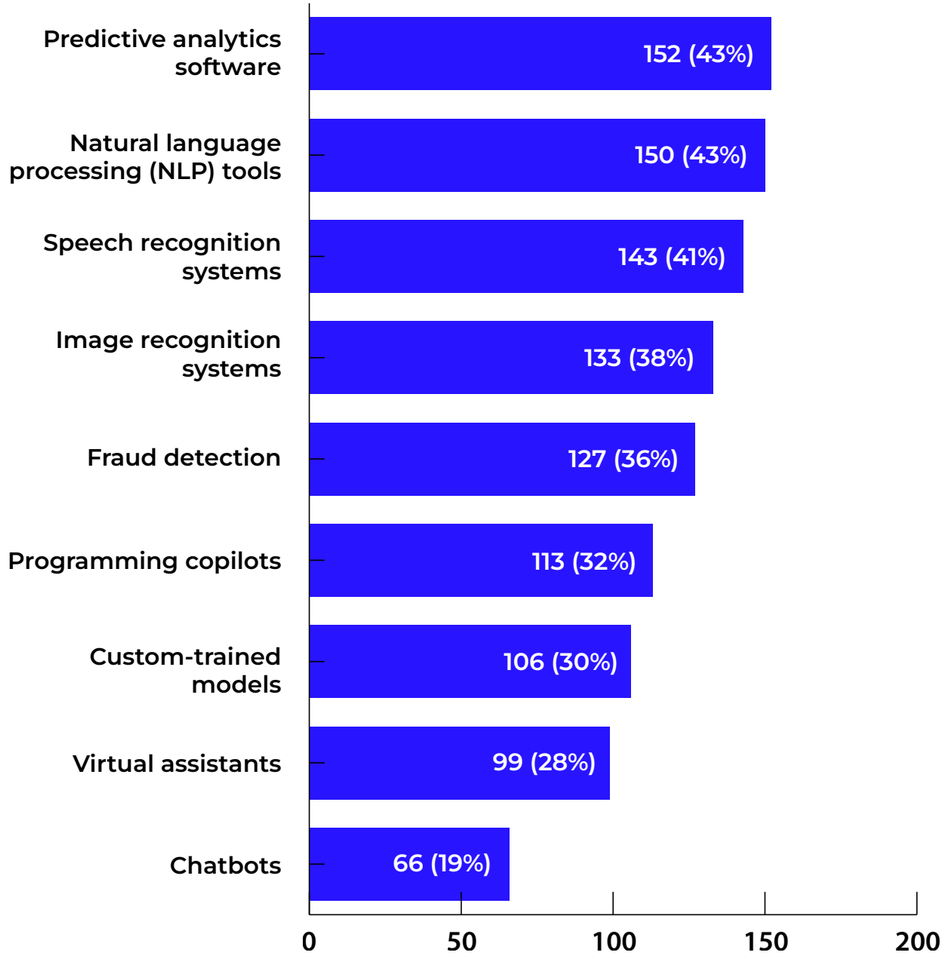
For CISO respondents' organizations using GenAI:

What cybersecurity processes/technologies are currently being enhanced/augmented by the use of GenAI?



For CISO respondents' organizations using AI:

What traditional AI platforms are currently used?

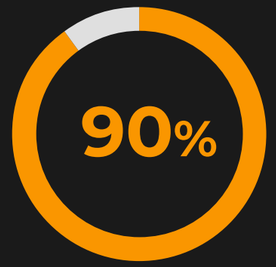


Section two

The Evolving Role of the CISO

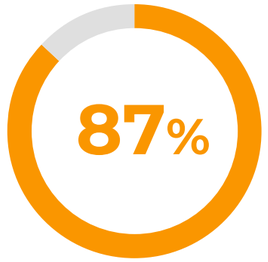
Organizations rely heavily on the CISO role for the adoption and implementation of AI. 54% of CISOs identified the CISO role as being primarily responsible for maintaining the security and compliance of the technology adopting AI. They expressed they're personally accountable for a range of issues, including cybersecurity budget allocation, cyberattack incidents, technology procurement, and vendor and third-party risk management. CISOs are also engaging more than ever now with the board, *half reported* to be meeting with their board at least quarterly, highlighting the increased level of liability on the role.
The introduction of GenAI to these sectors has increased the day-to-day stress of CISOs across industries, with Public sector CISOs reporting the highest stress levels due to their daily operations being affected by the complexities of managing sensitive data in an environment slower to adopt AI practices. The role of the CISO has become more essential than ever as they face challenges at an unprecedented scale.

There is also increasing liability with the CISO role, with high-profile cyber breaches becoming a part of the daily news cycle, heightening the public profile of CISOs and, in turn, placing them under intense scrutiny. Large scale incidents such as SolarWinds and Colonial Pipeline have eroded public assurance in organizations' abilities to secure critical data. In the case of SolarWinds, the company's CISO was charged with fraud by the SEC. The case resulted in *a shift* towards the CISO role, essentially acting as a risk officer for their organization and placing liability on a single role.
The introduction of AI and GenAI into these organizations has also brought increased scrutiny of CISOs, and 90% of respondents agree it has exposed them to increased liability in their role.

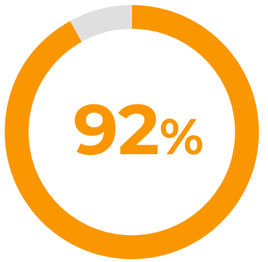


90% of CISOs feel they are exposed to increased liability as a result of AI/GenAI

90% of CISOs are finding themselves under increased pressure

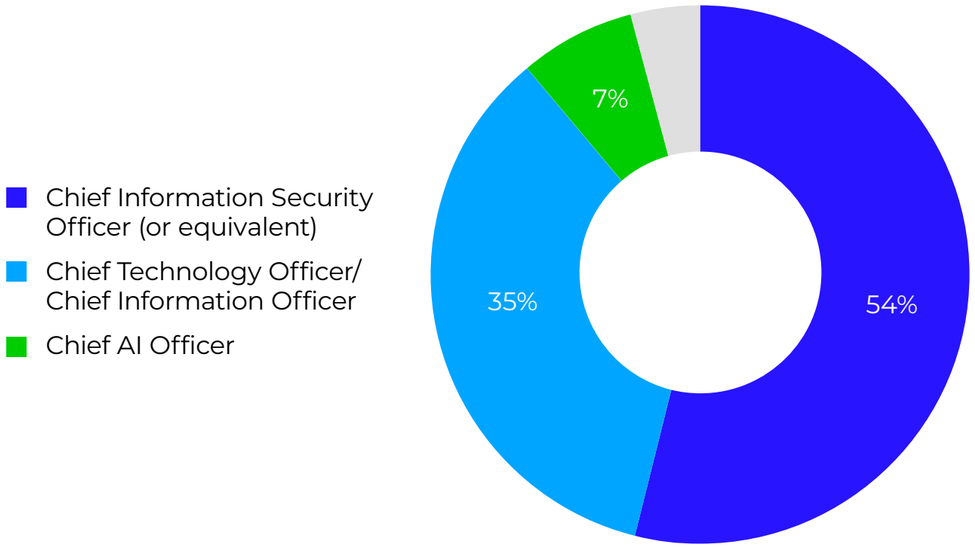


87% of CISOs regularly work outside of their contracted hours



92% of CISOs agree AI/GenAI has made them contemplate their future as a CISO

Primarily responsible for maintaining the security and compliance of technology adopting AI

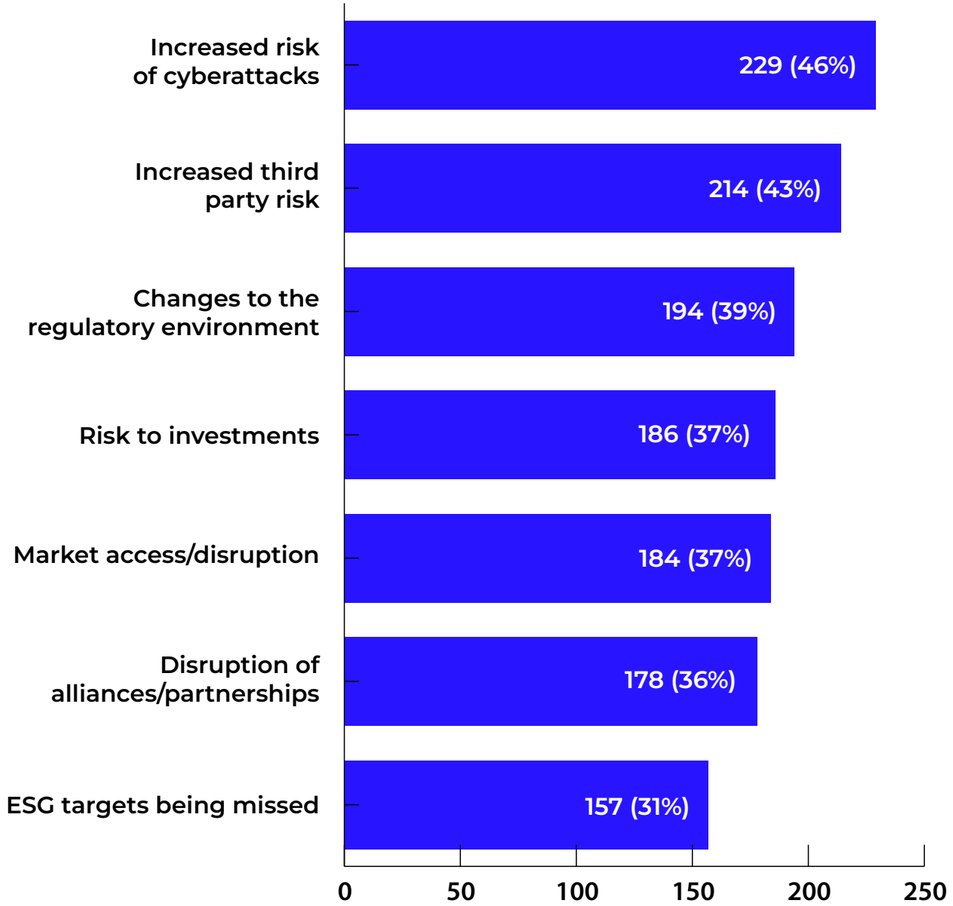


The changing regulatory landscape around AI and the commercial adoption of GenAI brings into question how well-equipped CISOs and their organizations are to adapt to these shifting policies and external factors. Overall, 97% of respondents are concerned about the shifting regulations over the use of AI, with one of the primary areas of concern being the use of AI to embolden nation-states to plant advanced persistent threats (APTs) within their infrastructure. The effect of the geopolitical landscape was also an area of concern, with 46% of overall respondents fearing an increased risk of cyberattacks if these external threats persisted. This topic was a pressing issue expressed by the IT, technology, and telecoms sector surveyed, with 63% of its CISOs expressing they were very concerned by the threat of malicious nation-state actors. Regulators must work closely with this sector to identify their perceived threats and work with industries to protect systems from APTs. CISOs themselves also believe they need to be better prepared to withstand these shifting threats and 100% agree they would face impacts as a result of changes to the geopolitical landscape.

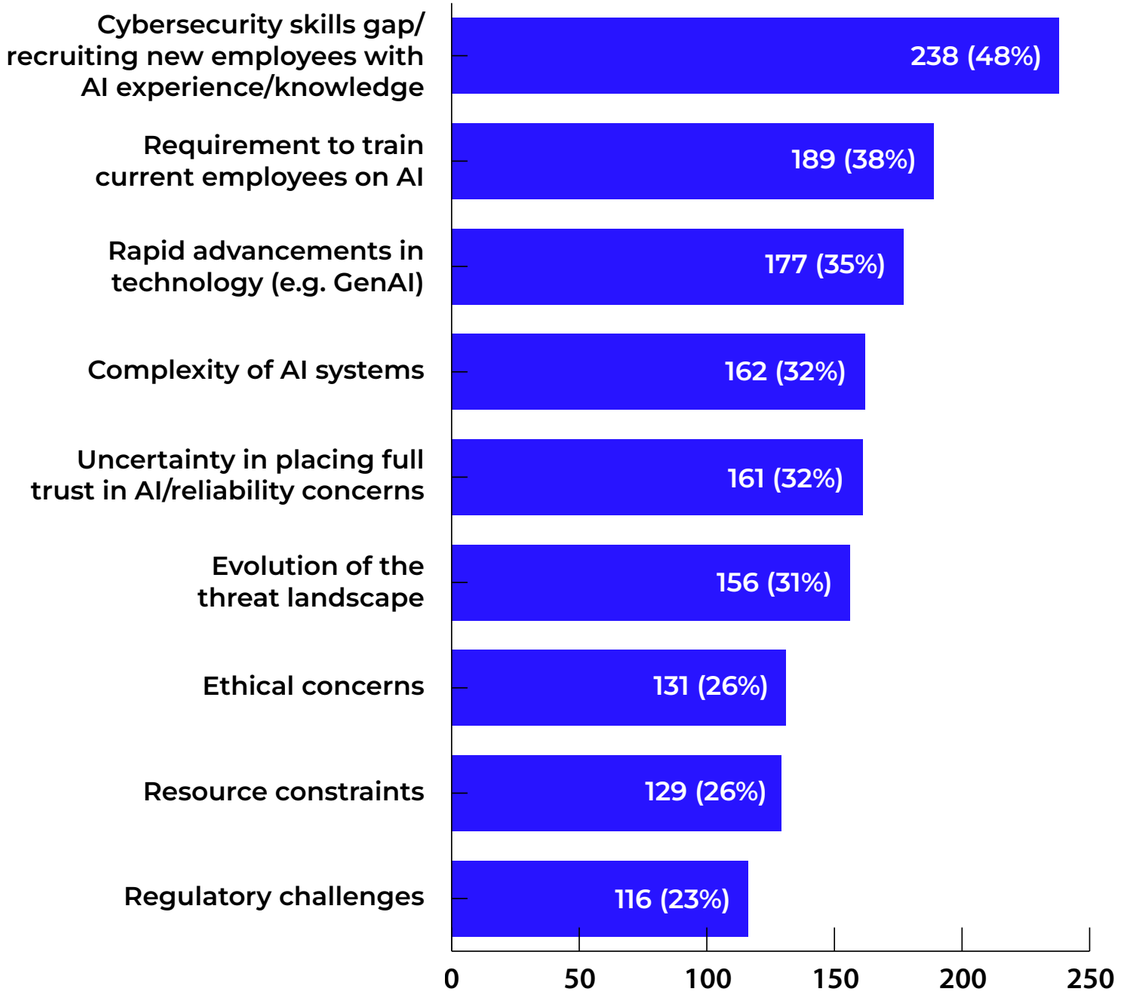
97% of CISOs are concerned about the shifting regulations over the use of artificial intelligence

An overwhelming number of CISOs (92%) expressed AI and GenAI have made them contemplate their future in the role, bringing into serious question how policy and regulation need to adapt to bolster the role of the CISO and enable organizations to secure their systems effectively. The primary driver of increased stress levels is the cybersecurity skills gaps and the need to recruit new employees with AI experience and knowledge (48%), and 38% of CISOs reported increased stress levels over the requirement to train current employees on AI. The rapid advancement and adoption of GenAI and other innovative technologies are of key concern to CISOs. However, current demanding workloads see 91% of CISOs expressing they don't have enough time to focus on the threat of these technologies, with 87% already regularly working outside of contracted hours.

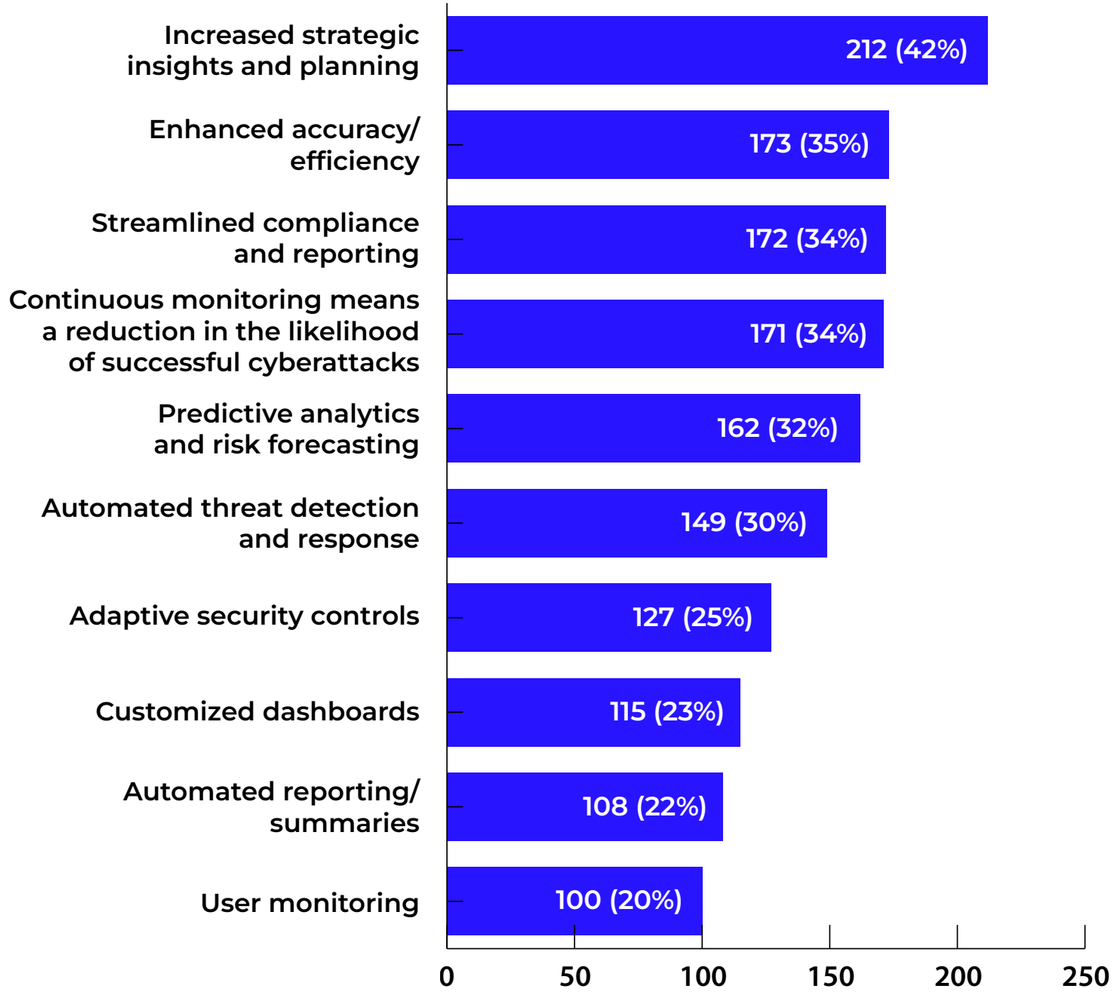
What impact, if any, would changes to the geopolitical landscape have on your organization?



How has artificial intelligence/GenAI increased your stress levels?

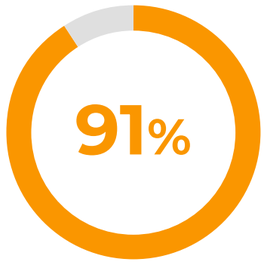


How has artificial intelligence/GenAI eased your stress levels?



Given the increase in stress and challenges CISOs face, organizations need to prioritize providing individuals with adequate support and resources. Considering the high liability and concentration on an individualized role, organizations need to foster cybersecurity awareness at all levels and train a well-informed workforce to act as a line of defense. CISOs have also expressed optimism about AI and GenAI's potential in cybersecurity. In some instances, AI has helped alleviate the stress of certain jobs CISOs have taken on, with 42% indicating it has eased stress levels through increased strategic insights and planning. This showcases the dual possibilities AI offers both CISOs and their organizations, where an increased AI-focused workforce can have beneficial impacts.

As the CISO role evolves to include additional responsibilities, they are now more regularly communicating with boards, with 89% of CISOs saying board members are increasingly asking them to attend meetings. 91% agree GenAI has the potential to streamline reporting when presenting to board members, and 92% of respondents agree GenAI has the ability to anticipate and address the concerns of board members.



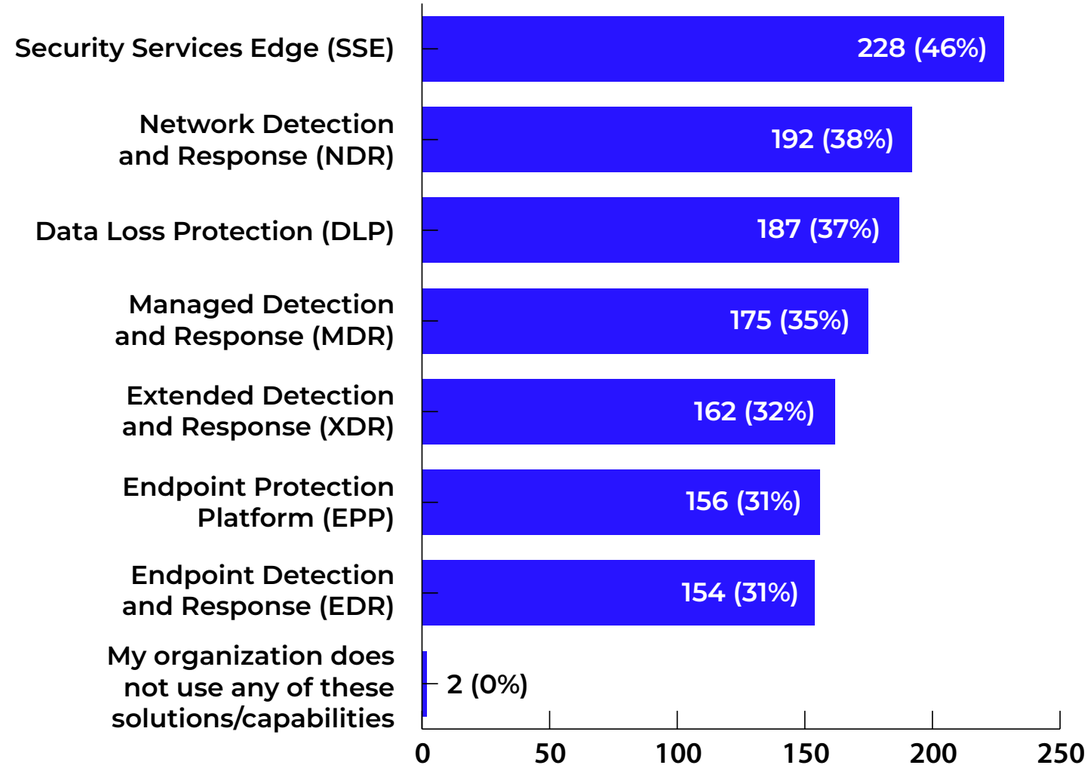
91% of CISOs report GenAI has the potential to streamline reporting when presenting to board members

Section three

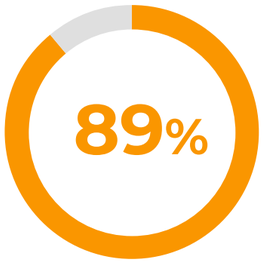
AI and Adaptability

CISOs have also recognized the potential for GenAI to better strengthen and prepare their organizational cybersecurity measures. All respondents currently using GenAI believe it has the ability to enhance/augment cybersecurity processes and technologies. This technology is being leveraged in areas such as security content creation, security testing/analytics, and incident response and forensics. In the future, most respondents anticipate GenAI will be integrated in Security Services Edge (SSE), Network Detection and Response (NDR), and Data Loss Prevention. These integrations could lead to more advanced and efficient security measures, including real-time threat detection, enhanced data protection, and more robust security frameworks. By incorporating GenAI in these areas, CISOs hope to stay ahead of evolving cyber threats and ensure better security for their data and networks. Almost half of CISOs are already working to secure their AI tools, with 45% of respondents reporting developing an AI committee to review AI tools and implementing governance, including security frameworks and standards.

Which of the following solutions/capabilities, if any, will your organization integrate GenAI functionality for over the next 12 months?

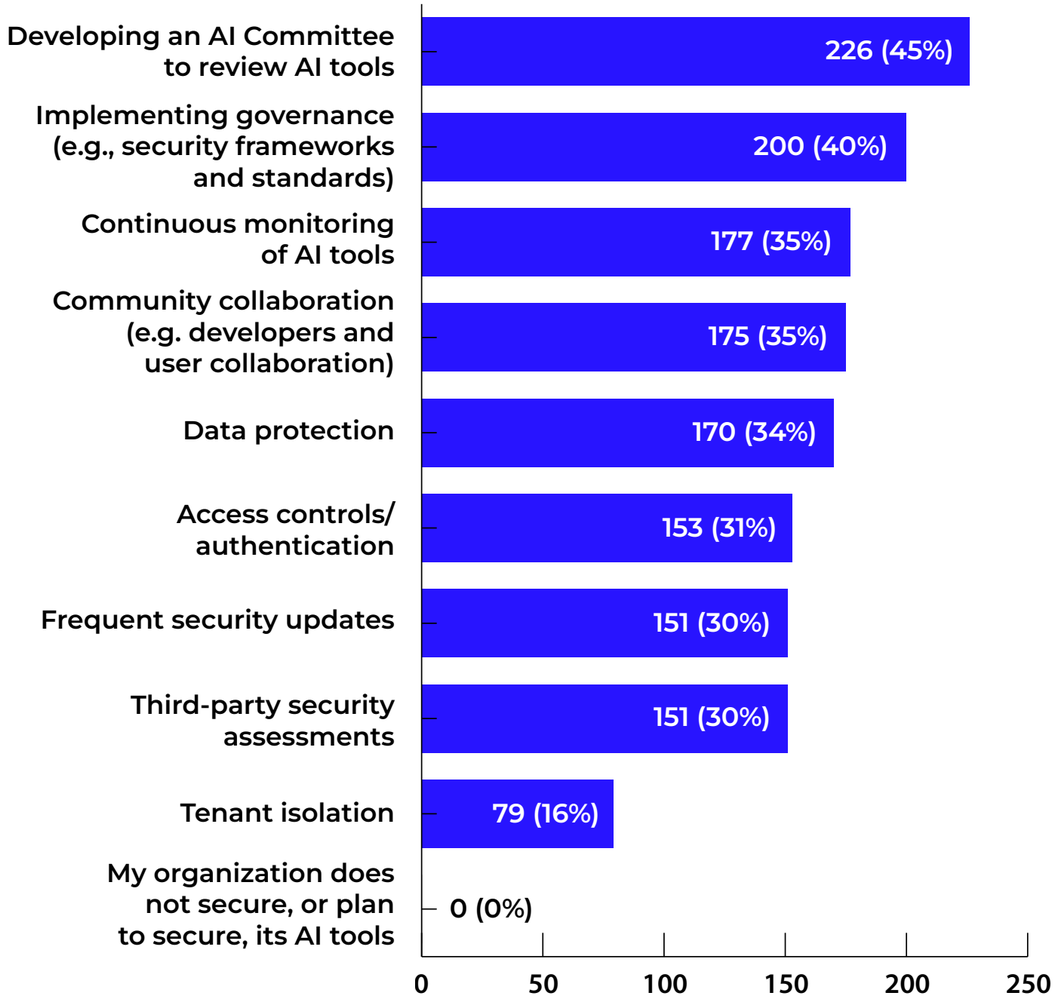


In addition to providing technical advantages in cybersecurity, most CISOs believe GenAI could provide an advantage to some extent in staffing and productivity, with 89% agreeing the adoption and integration of GenAI tools will help address SecOps staffing issues within their organization. Information sharing between organizations also provides an opportunity to help secure workforces, with 47% of respondents saying industry peers sharing GenAI insights and best practices was the most effective way to improve confidence in their workforce abilities to counter GenAI-produced cyberattacks. The automation of the workforce has become a point of concern in AI implementation and legislation, with regulators worrying about its effect on job loss. However, survey respondents all agreed if GenAI made SecOps roles redundant they would be repurposed within the organization, with a focus on managing and overseeing GenAI tools. The benefits of GenAI should not be ignored at all and clearly provide a double-edged sword to those in the security operations of organizations who are both concerned by its threat but also have promise in its benefits.



89% of CISOs agree the adoption/integration of GenAI tools will help address SecOps staffing issues within the organization

How does your organization secure, or plan to secure, its AI tools?



Recommendations:

GenAI provides both an array of challenges and promises to organizations and their CISOs. By recognizing threats, training workforces, and adopting measures to secure systems GenAI has the opportunity to enhance existing lapses in cybersecurity protocols and better protect organizations. Regulators should work with organizations and their CISOs to develop better legislation and address gaps in funding, access, and security across all sectors.

- **Increase funding and resources and tailor sector-specific regulation:** CISOs in public sector organizations particularly need increased funding and resources to support the adoption and implementation of GenAI. These need to extend to investments in technological infrastructure as well as training skilled personnel. However, all regulations should be widely applicable across various industries to facilitate compliance and enable technology companies to develop scalable solutions for global adoption.

- **Improve regulation and compliance:** As policymakers work to establish AI regulatory rules, there also needs to be clear compliance standards focused on concrete and measurable outcomes for sectors to adhere to, providing guidance for CISOs who stand to be the most liable for lapses in security and compliance measures.

- **Strengthening security frameworks:** Stakeholders should encourage the funding and adoption of integrating GenAI to enhance existing security measures, including Extended Detection and Response (XDR), Security Services Edge (SSE), Network Detection and Response (NDR), Data Loss Prevention (DLP), and real-time threat detection.

- **Increased data privacy and protection:** 55% of respondents indicated data privacy and protection require greater levels of regulation in the use of AI. CISOs are concerned about protecting the sensitive data of their organizations, particularly those in the public sector, and regulation needs to focus on greater protection of data privacy by passing federal privacy laws to ensure their operational security.

Additional Resources

- *Trellix XDR Platform:* Reduce risk, cost, complexity, and time to value with a single, open, comprehensive GenAI-powered XDR platform.
- *Trellix Wise:* Enabling customers with Generative Artificial Intelligence (GenAI)-powered security operations, Trellix Wise extends across the Trellix XDR Platform to automate and accelerate workflows and improve incident response, threat detection, prevention, and remediation.
- *Soulful Work*: Cybersecurity provides an opportunity to do meaningful, soulful work. Explore solutions for tackling the cyber talent gap and increasing diversity in cybersecurity.
- *Trellix Advanced Research Center Digest:* Subscribe to get the latest cybersecurity trends, best practices, security vulnerabilities, and more.
- *Mind of the CISO Research (April 2023):* To get inside the minds of today's security leaders, Trellix engaged with over 500 CISOs from around the world to understand their struggles and SOC challenges. Dive in for illuminating stats, real-life quotes, and learnings from security executives.
- *Mind of the CISO: Behind the Breach Research (November 2023):* Over 500 security executives share their experience managing a major cybersecurity incident and learnings for the best route forward.
- *The CISO's Guide to Ransomware (eBook):* When it comes to ransomware, every minute counts. Get road-tested guidance for CISOs and cybersecurity leaders to combat ransomware.

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 40,000 business and government customers with living security.

More at *www.trelllix.com*
Follow Trellix on *LinkedIn* and *X*.

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and major markets.

More at *www.vansonbourne.com*

Established in Washington D.C., over 60 years ago, The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decision makers chart a course toward a better world.

More at *CSIS | Center for Strategic and International Studies*.