



The AI security balancing act: From risk to innovation

A CISO's guide to mastering the risk
and potential of AI

Contents

03	Foreword
04	Is your cybersecurity strategy ready for the AI era?
07	Understanding AI-related risks
09	AI and security: CISOs must balance opportunity and risk
13	How CISOs can manage AI-related risks
19	How NTT DATA protects you on your AI journey
20	About the research
21	About NTT DATA

Foreword



Are CISOs prepared to help their organizations tap into the potential of AI while also protecting their digital assets from the risks that come with it? We call this the AI security balancing act.

Soaring investment in AI is already transforming industries and fundamentally changing the way we live, work and do business.

In fact, according to NTT DATA's Global GenAI Report, 95% of C-suite leaders say that GenAI is driving a new level of innovation in their organizations.¹

However, the increasing adoption of AI goes hand in hand with new and evolving cyberthreats, and AI-enhanced malicious attacks are a prominent emerging risk for organizations.

Encouragingly, the vast majority of organizations plan to spend more on both AI and security.

Our data shows nearly all C-suite executives (99%) are planning further GenAI investments until 2026, and 94% of the C-suite — including 95% of CIOs and CTOs — say GenAI has led, or will lead to, their organizations investing more in security.²

This underscores the acknowledgment by CISOs globally of changing imperatives in the age of AI. They need a modern, integrated cybersecurity posture to navigate this complex and fast-changing technology and business landscape.

But are CISOs prepared to help their organizations tap into the potential of AI while also protecting their digital assets from the risks that come with it? We call this the AI security balancing act.

In the pages that follow, we draw on insights from our GenAI report and other research to explore this dynamic and show how CISOs can navigate the risks and opportunities posed by AI.

From evolving regulations to the shifting dynamics of decision-making, we examined the views of 2,300 respondents from 34 countries and 12 industries, as detailed in our GenAI report. We offer insights into the challenges and vulnerabilities introduced by AI and GenAI, along with guidance on how to proactively integrate security into AI initiatives from the very beginning.

This guide aims to help CISOs understand how to help their organizations mitigate the threats of AI while leveraging cybersecurity as a business advantage in an era of unprecedented change and opportunity.

Now is the time for CISOs to assess whether their organizations' current cybersecurity strategy is robust enough to address the sophisticated, AI-enhanced threats of today and tomorrow — and to develop a proactive plan of action.

Join us as we share our insights on how to prepare your enterprise for a more secure and advantageous AI-driven future.

Sheetal Mehta

Senior Vice President and Global Head of Cybersecurity,
NTT DATA, Inc.

^{1,2} NTT DATA's Global GenAI Report, November 2024

Is your cybersecurity strategy ready for the AI era?

In 1956, the term “artificial intelligence” was coined at the [Dartmouth Conference](#), marking the formal beginning of AI as a distinct academic discipline. It is only in the past two decades, however, that AI has become more accessible to a broader range of organizations — helped along by rapid and significant advances in machine learning, natural language processing, data storage and computing power.

Today, AI and GenAI have the potential to reshape entire industries and transform organizations into highly efficient, competitive and profitable business leaders.

CEOs' views on AI and GenAI

89%

of CEOs identify AI as the top technology they need to ensure their competitiveness and profitability.

Source: WSJ Intelligence & NTT Global Study
November 2024

99%

of CEOs are planning further GenAI investments, while 2 in 3 are planning significant investments in the coming two years.

Source: NTT DATA's Global GenAI Report,
November 2024

94%

of CEOs say GenAI has caused them, or will cause them, to invest more in cybersecurity.

Source: NTT DATA's Global GenAI Report,
November 2024

In fact, our data shows that nearly every organization worldwide intends to keep investing in GenAI, with 89% of CEOs identifying it as the top technology they need to ensure their competitiveness and profitability, and 2 in 3 planning significant investments in GenAI in the coming two years.³

There is also a growing recognition that increased investment in GenAI necessitates a corresponding commitment to cybersecurity, with 94% of CEOs (and 95% of CIOs and CTOs) saying they are already spending more on security or that they plan to do so.



³ NTT DATA's Global GenAI Report, November 2024

Transforming business across industries: The potential of GenAI

Our Global GenAI Report shows that 97% of CEOs expect a material impact from GenAI. The surge in popularity of large language models (LLMs) like ChatGPT and Gemini has added impetus to the rise of GenAI, and we've only just scratched the surface of the full business value this technology can deliver.

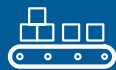
The possibilities are infinite: Just about anyone can use natural language to interact with these tools and generate text, images, code, music and more, even if they have no technical knowledge.

There is also now enough online content to act as training data for LLMs, while cloud computing is providing ever more powerful, scalable and cost-effective infrastructure to support these models.

As a result, the potential of GenAI in particular is rapidly becoming a reality for organizations across industries.



In healthcare, the technology is revolutionizing patient care and research by enabling the analysis of vast amounts of medical data to identify patterns and predict patient outcomes.



In manufacturing, GenAI is helping to streamline production processes and supply chain management. By predicting maintenance needs and reducing production downtime, it helps manufacturers work more efficiently and with a greater degree of reliability.



In financial services, it is enabling the transformation of risk management and fraud detection, making these processes more accurate and responsive. Additionally, AI-powered chatbots are ushering in a new era of customer service by providing fast, personalized support to customers.

“ As GenAI continues to evolve, its impact on these and other industries will only become more significant.



Progress comes with new security risks

AI is also being widely used to implement advanced automation and analytics in threat detection and security operations. Initial applications of AI in security include automating simple tasks like phishing detection and evidence gathering; as the technology evolves, it will allow organizations to automate how they detect and respond to an ever wider variety of threats, significantly reducing the time between identification and mitigation.

Indeed, many organizations list improved security as one of the top three outcomes they have seen as a direct result of their GenAI deployments.⁴

88%

of organizations are very concerned about the potential security risks associated with GenAI deployments.

Source: NTT DATA's Global GenAI Report, November 2024

Only 24%

of CISOs strongly agree that their organization has a robust framework for balancing risk with value creation.

However, the rapid adoption of AI and GenAI has also exposed new attack surfaces, unexpected security vulnerabilities and sophisticated, AI-enabled threats.

Cybercriminals are exploiting inadequate security controls to manipulate AI models and compromise data integrity and the reliability of AI-enabled solutions. This is why 88% of organizations are very concerned about the potential security risks associated with GenAI deployments.⁵

Our data also shows that just 24% of CISOs strongly agree that their organization has a robust framework for balancing risk with value creation when it comes to implementing GenAI.⁶

To protect the large volumes of data being created in the era of AI and GenAI, organizations need policies and controls that allow them to continuously assess and mitigate the associated security risks. They have to secure their supporting infrastructure and find a way of keeping business operations going when threats arise.

Next, let's explore the different types of AI-related risks and how to manage them.



^{4,5,6} NTT DATA's Global GenAI Report, November 2024

Understanding AI-related risks

Malicious actors are manipulating advanced AI to launch complex and evasive attacks. For instance, they are using AI to create highly convincing phishing emails and automate the process of finding and exploiting vulnerabilities in software. On a broader scale, AI has the potential to be used in cyberwarfare and state-sponsored attacks.

Cybercriminals also know that AI systems rely on the quality of their underlying data and algorithms, and will often probe these areas for vulnerabilities. Threats to these systems include:

- **Adversarial attacks**, which involve manipulating input data to deceive AI algorithms
- **Data poisoning**, which entails tampering with the training data of AI systems
- **Algorithmic bias**, which can result in discriminatory outputs and undermine trust in these systems

CISOs need to take a proactive, well-considered approach to mitigating the risks associated with AI — but there are hurdles to overcome. For example, just 44% of the C-suite agree they have the systems in place to manage privacy risks that could expose an organization to threats from data poisoning.⁷

Just 44%

of the C-suite agree they have the systems in place to manage privacy risks that could expose an organization to threats from data poisoning.

Source: NTT DATA's Global GenAI Report, November 2024



⁷ NTT DATA's Global GenAI Report, November 2024

Data management, GenAI and agentic AI

Many organizations have only just started grappling with GenAI-related data management — a crucial component of AI security, as it keeps the data used to train and operate AI and GenAI systems accurate, secure and compliant with regulatory requirements.

However, these efforts are intensifying: While only 53% of organizations have already assessed their data-readiness as part of laying the foundation for secure and trusted GenAI (including data platforms and management), 95% expect to have done so by the end of this year.⁸

Beyond the data itself, GenAI also introduces potential security vulnerabilities through its complex and advanced algorithms. These models have millions of parameters that are constantly changing, making it difficult to predict and control the behavior of the models and increasing the risk of unintended consequences.

The emergence of agentic AI

Agentic AI is the current frontier of innovation, facilitating complex decision-making and troubleshooting across organizational domains, including cybersecurity.

In cybersecurity, agentic AI surpasses traditional rule-based automation in its ability to autonomously detect, analyze and respond to threats in real time — with intent and context awareness. It can adapt dynamically to shifting attack tactics while orchestrating multiple tools and workflows for faster threat triage and remediation.

For the CISO's security team, this means less alert fatigue and more analysis capacity despite any workforce shortages. Ultimately, agentic AI acts as a force multiplier that strengthens defenses against increasingly complex cyberattacks.

However, agentic AI will only add this value if it is guided by well-defined data governance and privacy policies. For example, deploying unrestricted AI agents — such as note-taking assistants that participate in virtual meetings — can be risky. Without proper oversight, these agents can access confidential information for unintended purposes or even leak it into the public domain.

NTT DATA's insights show that large enterprises are still 18 to 36 months away from fully integrating these technologies into their production environments, and the C-suite — CISOs in particular — has a considerable task ahead in preparing for a secure future powered by agentic AI.

Only when organizations fully grasp the importance of robust, continuous data management in an environment of relentless AI innovation will they truly be able to reap the benefits of their investments in these technologies.

The agentic frontier

Agentic AI refers to AI systems capable of autonomous action, with AI agents that can collaborate and complete complex workflows with minimal human supervision. They can understand context, set goals, reason through subtasks and adapt their actions based on changing conditions.



⁸ NTT DATA's Global GenAI Report, November 2024

AI and security: CISOs must balance opportunity and risk

CEOs and the wider C-suite are optimistic about the ability of their AI-led technology portfolio to make their organizations more profitable, as they see the potential of AI to improve business operations and outcomes.

Yet, despite this optimism, there is a notable disconnect between the strategic goals of the C-suite and the operational hurdles faced by CISOs, 97% of whom identify themselves as primary decision-makers in GenAI.⁹

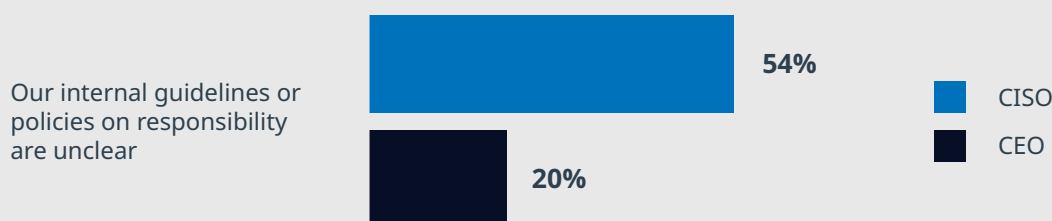
They are tasked with maintaining security, privacy and compliance in AI deployments — all critical to business success — yet they don't feel they are in control when it comes to embracing these new technologies.

While CISOs are just as eager as their C-suite peers to embrace AI, they bear the unique responsibility of mitigating the associated risks in a fast-evolving and mostly unregulated environment.

- These risks include **exposing the vast amounts of sensitive data** that AI systems need to function effectively — data that may include personally identifiable information and financial records, for example. Unauthorized access, data breaches and data misuse spell disaster for any organization.
- There is also a **lack of clear strategies and policies** amid the rapid pace of AI innovation, with new algorithms, tools and techniques constantly emerging. For example, more than half of CISOs (54%) say internal guidelines or policies on GenAI responsibility — deploying GenAI systems securely, ethically and in compliance with regulations — are unclear, yet only 20% of CEOs share the same concern. Also, 72% of organizations we surveyed still lack a formal GenAI usage policy.¹⁰
- Moreover, **regulatory frameworks for AI are still in their infancy**. Many countries and industries lack specific regulations that address the unique security and privacy concerns of AI. Our research also shows that 82% of organizations find government regulation of AI to be unclear, which stifles innovation and hinders investment in GenAI due to the associated uncertainty.¹¹ Without clear regulatory guidance, CISOs must often rely on their own expertise and industry best practices instead.

Views on internal guidelines and policies

CISOs versus CEOs: Do you agree that your organization's internal guidelines or policies on responsibility are unclear?

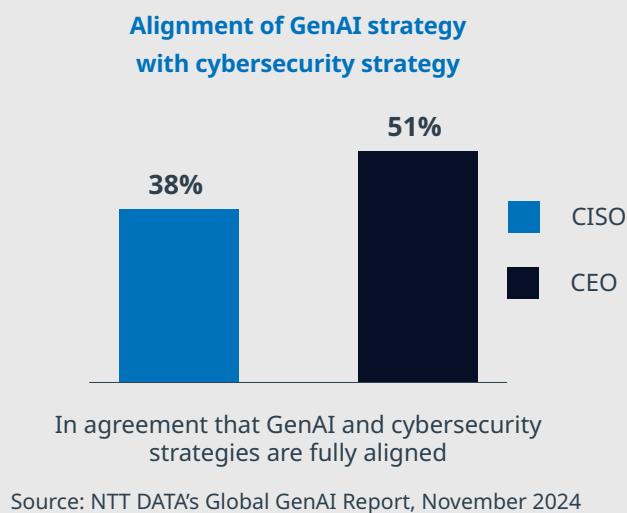


Source: NTT DATA's Global GenAI Report, November 2024

Further proof of the misalignment at the executive level is that in organizations that prioritize innovation over responsibility in implementing GenAI, 71% of CISOs (versus just 42% of CIOs and CTOs) cite “a lack of clear direction from leaders on how to maintain responsibility”. Adding to the challenge, 69% admit that their teams lack the skills to work with this fast-evolving technology.¹²

Only 38% of CISOs compared with 51% of CEOs agree there is alignment between GenAI and cybersecurity strategies, and nearly 90% of CISOs say they are very concerned about the potential security risks associated with GenAI deployments.¹³ Additionally, just 1 in 3 strongly agree that the security risks are adequately understood and managed within their organizations.

Fewer CISOs than CEOs agree that there is alignment between their organization's GenAI and cybersecurity strategies. Without such alignment, the risk to data security and privacy increases.

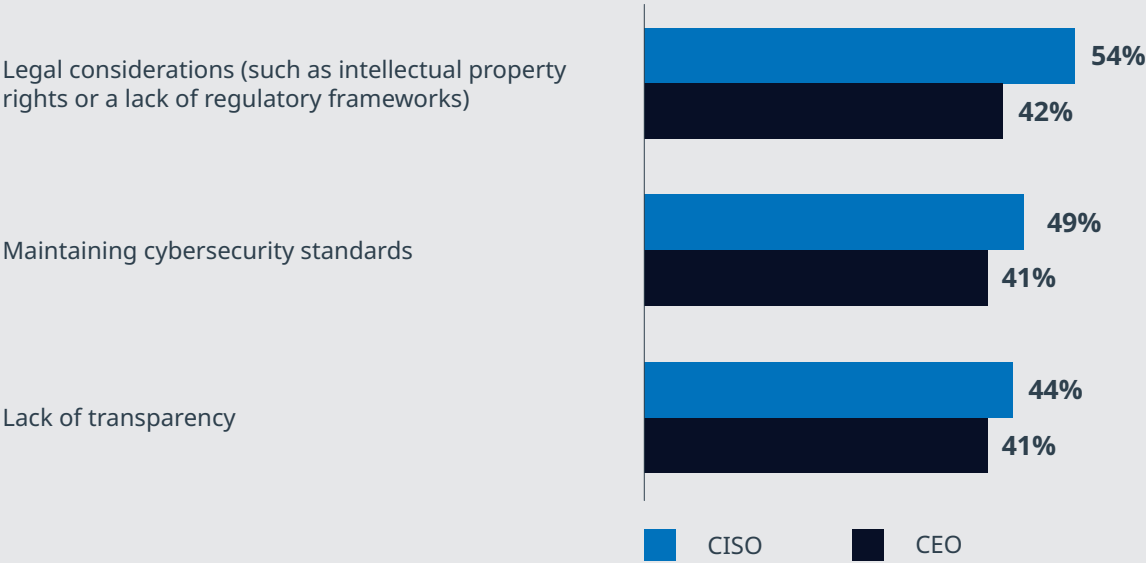


Furthermore, CISOs are 46% more likely than the rest of the C-suite to be uncomfortable with opaque decision-making algorithms and the “black box” nature of some GenAI models — and their concerns don’t end there.¹⁴

They are also more likely than CEOs to have trust issues when it comes to the adoption of GenAI, especially regarding legal considerations (such as intellectual property rights or a lack of regulatory frameworks), maintaining cybersecurity standards and a lack of transparency.

^{12,13,14} NTT DATA's Global GenAI Report, November 2024

Trust issues affecting organizations' adoption of GenAI



Source: NTT DATA's Global GenAI Report, November 2024

These challenges are compounded by aging, absent or unintegrated infrastructure: 46% of CISOs cite infrastructure complexity as their most common GenAI challenge, while 87% believe that legacy infrastructure is holding back their GenAI progress. Legacy systems also make it harder to gain visibility of AI usage across an organization.

Additionally, 8 in 10 CISOs say the cloud environment is the optimal infrastructure for the efficient and cost-effective scaling of GenAI initiatives. However, only 45% of organizations strongly agree they have conducted a detailed analysis or assessment of their future infrastructure needs to support GenAI.¹⁵



¹⁵ NTT DATA's Global GenAI Report, November 2024

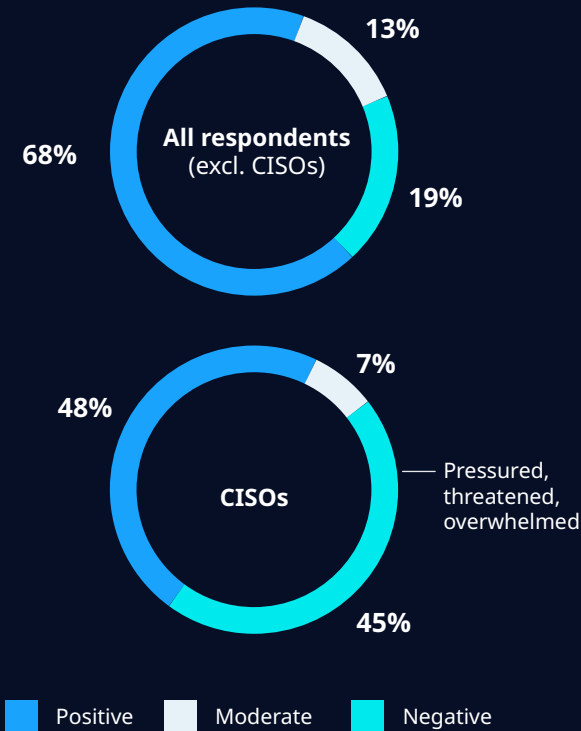
CISOs are clearly in uncharted territory; unsurprisingly, almost half (45%) express negative sentiments toward GenAI adoption, saying they feel pressured, threatened or overwhelmed. Notably, only 19% of all other respondents share this outlook.¹⁶

Given the myriad challenges and concerns we have outlined, it is understandable that CISOs are taking a cautious, step-by-step approach to AI adoption as they try to strike a balance between the innovation potential of AI and the need for caution and responsibility.

Despite being circumspect about the deployment of GenAI, security teams acknowledge its business value. In fact, 81% of senior IT security leaders with negative sentiments still agree that GenAI will boost efficiency and improve the bottom line.¹⁷

In the next chapter, we will delve into the strategies they can follow to mitigate these risks.

Strongest sentiment on GenAI



^{16,17} NTT DATA's Global GenAI Report, November 2024

How CISOs can manage AI-related risks

To maintain security as AI adoption increases, CISOs should follow a multilayered approach that includes both technological and organizational measures.

This approach starts with working with other business leaders to formulate a clear business case for creating value with AI in their organization and understanding the essential elements needed for the implementation journey — whether for AI more broadly or for GenAI.

Here are six practical steps all CISOs can take to support their organizations in adopting AI securely, responsibly and competitively.

1

Improve observability

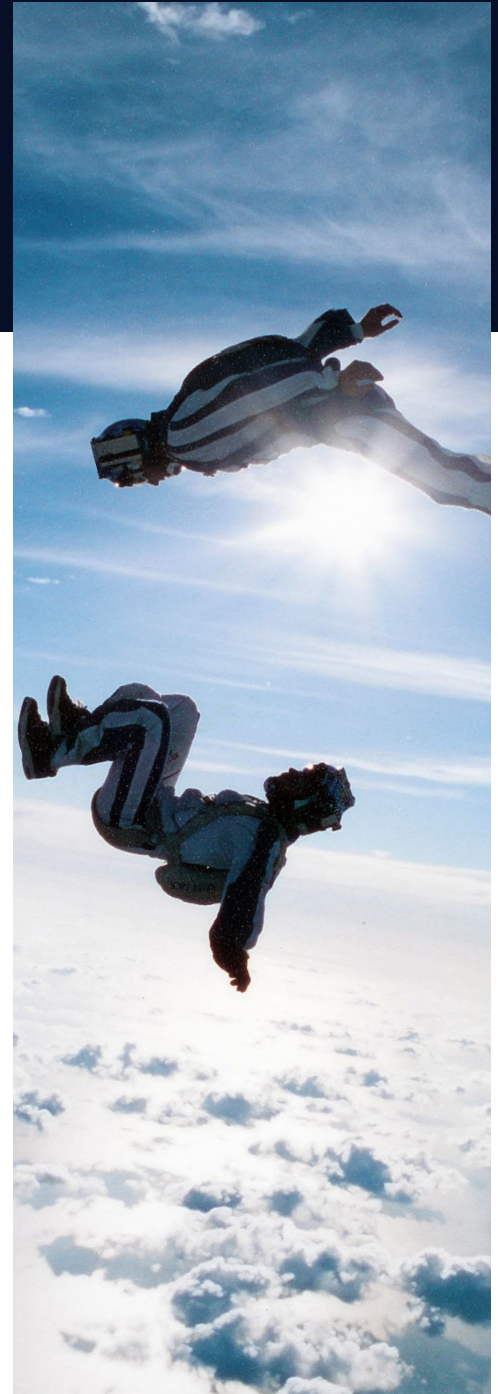
To address the risks associated with AI, you need to understand where and how it's being used. However, as AI becomes more deeply embedded in business operations, its usage and risks are increasingly difficult for CISOs to track.

As AI becomes more democratized, its growing popularity and the unofficial or “shadow” adoption of AI tools without the IT department's approval make it challenging for CISOs to gain an accurate overview of AI use within the organization. But it is only through such a comprehensive understanding that CISOs can fully grasp the risks AI introduces and develop effective strategies to manage them.

In this environment, you have to reimagine your approach to observability and adopt processes and tools suited for the age of AI.

Establish and maintain an inventory of AI assets and monitor the integration of AI into development pipelines to automatically log new models as they are created. Also, revamp your security operations center with a governance platform designed to oversee model usage and performance, including logging all AI model interactions.

Finally, collaborate closely with key departments in your organization, such as legal and IT, to share the responsibility of tracking and managing AI use.



2

Create an AI security policy

While you assess how AI is being used in your organization, develop a broad-based AI security policy framework that outlines procedures for mitigating AI-related risks and the methods for their implementation. Include straightforward guidelines and oversight mechanisms for the secure use of AI models and address compliance and legal considerations.

Organizations are facing significant confusion due to the absence of clear policies addressing the unprecedented nature of AI. You need a policy that extends your organization's broader governance, risk and compliance framework and provides clear guidelines on how to integrate AI technologies and tools securely.

This policy must be designed to enable innovation and progress, rather than impose excessive restrictions. It should also not be overly rigid, as such an approach would hinder its effectiveness.

To ensure adoption of the policy throughout your organization and address resistance to change, align it with your specific business strategies. Define clear roles and responsibilities, and keep the policy up to date as the AI landscape evolves.





3

Embed security by design

Security, privacy and trust are integral elements of AI systems and must be incorporated by design into your architecture, your data and the code itself.

Implementing measures such as access control, encryption and data anonymization can prevent unauthorized access and keep your sensitive data accurate, secure and tamper-proof.

Also, your business teams need to set out in detail why they need access to specific datasets, and how and when they will use these.

Focus on data protection

In an environment where LLMs are processing ever-increasing amounts of data and their ability to infer information from seemingly disconnected details grows by the day, you need to put in place data-protection measures adapted for the era of AI.

Your data controls should focus on securing your AI models and the data used to train them. Also consider measures like federated learning models, which allow AI training without the need to share sensitive information.

Implement model validation and testing

Invest in rigorous testing before deploying any AI or GenAI system so you can address any vulnerabilities early on.

Keep testing and validating regularly to keep pace with the latest advances in AI, and use techniques like adversarial training to make your AI models and data management systems more resilient to attacks. Combine this approach with industry-appropriate governance practices.

Facilitate integration and compatibility

While it can be complex and time-consuming to integrate your required AI security posture with your existing cybersecurity infrastructure, it's critical to focus on compatibility and interoperability between AI systems and your legacy technologies to avoid disruptions and maximize the effectiveness of AI in cybersecurity.

Even then, legacy technologies can expose new attack surfaces or hold back your latest security tools or AI-driven security approach. Consider moving to a modern security posture to secure your AI strategy. Combining disparate security technologies into a unified platform reduces gaps in security, enables automation and delivers efficiencies that lower the cost of your security operations.

Importantly, the introduction of an AI solution cannot be a ringfenced exercise. It must form part of your organization's technological DNA, with full awareness of the benefits and risks across all operations.

4

Ensure continuous monitoring and threat detection

Advanced monitoring tools and techniques allow you to quickly identify suspicious activities or anomalies in your AI systems. By detecting and responding to these threats in real time, you can mitigate risk and avert potential breaches before they cause real harm.

AI bolsters threat hunting and modeling by continuously analyzing your network traffic, the behavior of your users, and your system configurations to identify vulnerabilities. In [security operations centers](#), the technology is already changing how we detect and respond to cyberthreats.

Maintain an incident-response plan that includes procedures for detecting, containing and recovering from AI-driven attacks. It should be accompanied by a clear strategy for business continuity and incident recovery to minimize business disruptions in the event of a breach. This approach to cyber resilience needs constant updating because of the speed at which AI is developing.

Think of a manufacturer using AI in supply chain management to predict demand, streamline inventory and automate logistics. Their extended partner and vendor network creates multiple potential entry points for cyberattacks. AI can continuously assess the cybersecurity postures of all vendors and partners, as well as the data channels between them and the manufacturer. To further strengthen security, this capability can be complemented by an AI-driven incident-response system.



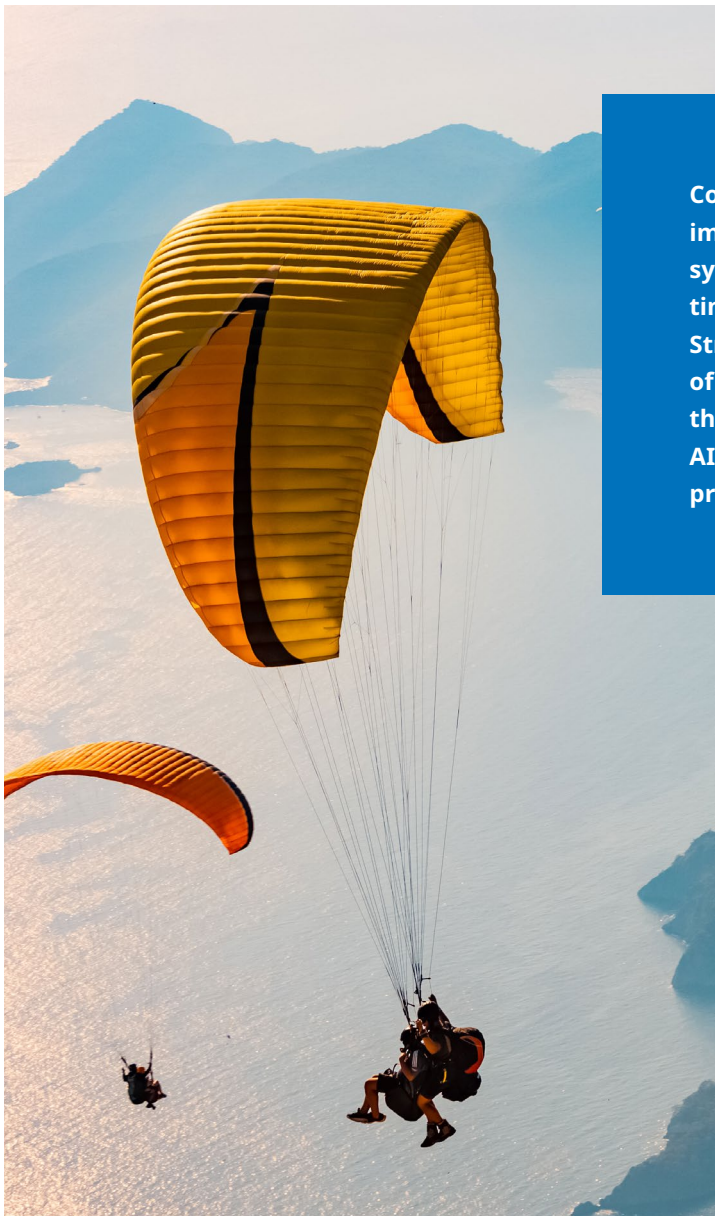
5

Understand risk management and compliance

AI governance is an evolving field, and some countries are ahead of others in this regard. In Singapore, for example, guidance on the safe and secure use of AI has been in place for some time.

Thoroughly study and follow frameworks that are already in place to assess whether your AI systems are not only effective but also responsible and compliant with international standards. These include:

- The [Artificial Intelligence Risk Management Framework \(AI RMF 1.0\)](#) of the US National Institute of Standards and Technology (NIST)
- The [ISO/IEC 42001:2023](#) standard that provides guidelines for managing AI systems in organizations
- The Open Web Application Security Project's [OWASP Top 10 for Large Language Model Applications](#)



Consider the example of a hospital implementing an AI-enabled monitoring system that analyzes patient data in real time to detect early signs of health issues. Strict regulations apply to the processing of patients' sensitive health data, so the system needs encryption and other AI-enabled security monitoring tools to prevent malicious activities.

Additionally, regular risk assessments are an important component of risk management, as they effectively identify potential vulnerabilities in your organization. The C-suite lists rigorous impact assessments and risk management, including legal, financial and security audits, as one of their top two priorities — second only to employee education — in GenAI development.¹⁸

You also need to understand the regulatory landscape around both your organization and your extended chain of vendors and partners, as attackers can access your systems through a third party, too.

¹⁸ NTT DATA's Global GenAI Report, November 2024

6

Encourage collaboration and education

When you're evaluating security frameworks for your organization, consider your specific AI use cases, business goals and industry regulations.

Both AI and security are here to enable your business. Foster collaboration between your security teams and AI developers to integrate security into the AI development lifecycle. Educate your employees about the risks associated with AI and the importance of following best practices in security.

In our GenAI research, C-suite executives ranked employee education and training on ethical GenAI use as the top responsibility for business leaders in developing GenAI. By building a culture of security awareness, you equip employees to become your first line of defense against potential threats.

However, security and AI resources are in short supply — so how do you access the expertise and innovation that will keep you one step ahead of cybercriminals? Working with a trusted cybersecurity partner will help you align your approach to AI-driven security with your business requirements.

CISOs opt for co-innovation in GenAI

CISOs' preferred approach to deploying GenAI solutions in the next two years is bespoke co-innovation with a strategic IT partner.¹⁹

However, while **64% of CISOs** support this approach, just **49% of organizations overall** — and **48% of CIOs and CTOs**, in particular — say the same.

These statistics point to CISOs being understandably cautious in their stance on GenAI deployment. Should anything go awry with GenAI solutions, they are the ones in the spotlight.

Once CISOs start assessing potential GenAI partners, their **main criterion** is an end-to-end GenAI service offering — in other words, full-stack capabilities. They are **48% more likely** than the rest of the C-suite to include this requirement as one of their top three selection criteria, alongside a potential partner's co-innovation skills and the depth of their industry experience and strategic partnerships. This is not surprising, given that **69% of CISOs** say their teams lack the skills to work with GenAI.

Additionally, CISOs list gain-sharing as their most preferred financial model for GenAI solutions, where the risks and benefits of a digital transformation project are shared among the parties involved.

¹⁹ NTT DATA's Global GenAI Report, November 2024

How NTT DATA protects you on your AI journey

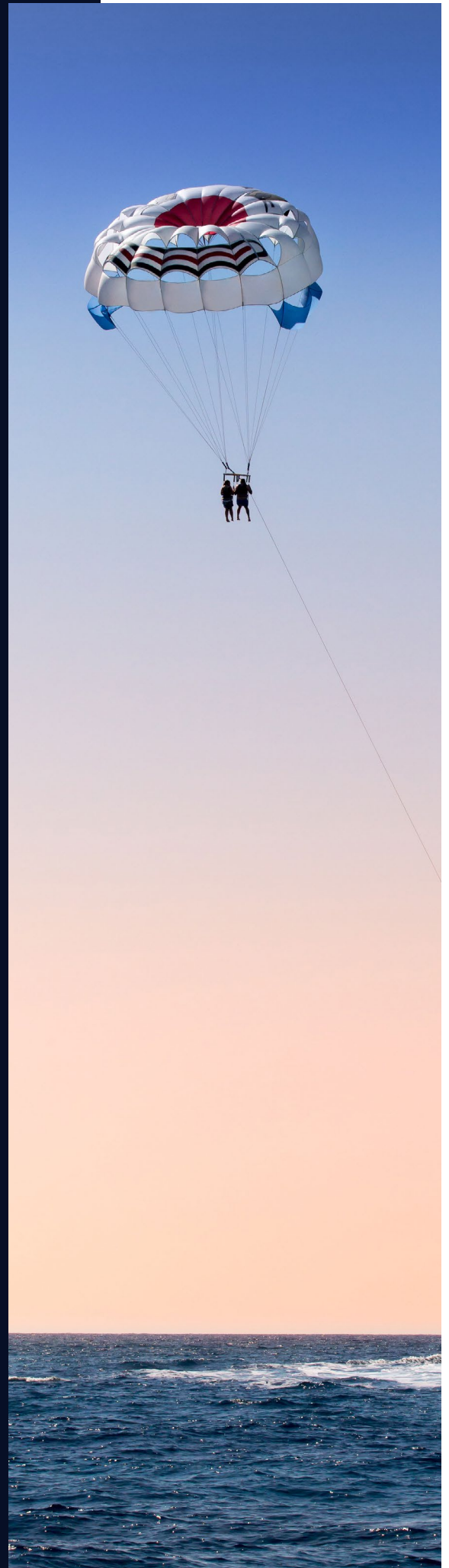
As you prepare to manage AI-related risks in your organization and assess your AI security maturity, NTT DATA empowers you to innovate safely with AI-driven solutions and secure your business growth:

- We use our robust AI trust framework and Cybersecurity Assurance Platform to continuously assess your cybersecurity maturity and AI risk, fostering responsible AI adoption and ensuring regulatory compliance.
- Our multilayered zero trust security solutions protect your organization's AI assets and mitigate risks during development and runtime. Moreover, our GenAI-enabled security operations centers rapidly detect and respond to AI-generated threats.
- Our Secure AI Lab service provides a turnkey experimental playground for rapid learning and strategizing.

NTT DATA's full-stack, full-lifecycle AI security services — from advisory and consulting to implementation and managed services — help organizations answer critical questions about safeguarding their AI journey.

Contact us

Get in touch with NTT DATA's AI and security consultants to discuss your approach to AI security. We will share practical insights based on industry trends, our global experience and local expertise, and our industry-leading investments in research and development.



About the research

NTT DATA's Global GenAI Report in numbers

- A balanced sample of 2,307 GenAI decision-makers (95%) and influencers (5%)
- Coverage spans 34 countries in five regions
- 12 industry sectors
- 74% of respondents from large enterprises with more than 10,000 employees
- 68% of participants were from the C-suite; 27% were at Vice President, Head of or Director level, and 5% were senior managers or specialists
- 42% of participants were in IT roles; 58% in non-IT roles

Research methodology

Global GenAI Report, November 2024

This report is based on independently sourced research data. Participants were selected via random sampling on the basis that they had a direct or indirect influence on their organization's GenAI requirements, or decision-making authority in that regard.

The research data was gathered via an online questionnaire that ran in September and October 2024. Research was conducted for NTT DATA by Jigsaw Research, an international strategic-insight agency with an exclusively senior team.

Data integrity, validation and analysis were performed by NTT DATA's specialist in-house Primary Research and Benchmarking Team in conjunction with Jigsaw Research. Data and outliers were validated in accordance with standard research-industry rules, disciplines and best-practice approaches. The data is presented at a 98% confidence level with a 3% margin of error.

Future-Ready Innovation: Strategies for 2025 and Beyond, January 2025

A global survey commissioned by NTT and conducted by WSJ Intelligence. The survey polled 351 global CEOs, representing US companies with annual revenues exceeding \$1 billion and non-US companies with revenues of \$500 million or more. The findings are presented in a white paper, **Future-Ready Innovation: Strategies for 2025 and Beyond**, which explores these trends in detail.



About NTT DATA

NTT DATA is a \$30+ billion global innovator of digital business and technology services. We serve 75% of the Fortune Global 100 and are committed to helping clients innovate, optimize and transform for long-term success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem of established and startup companies. Our services include business and technology consulting, data and artificial intelligence, industry solutions, as well as the development, implementation and management of applications, infrastructure and connectivity. We are also one of the leading providers of digital and AI infrastructure in the world. NTT DATA is part of NTT Group, which invests over \$3.6 billion each year in R&D to help organizations and society move confidently and sustainably into the digital future.



Visit nttdata.com to learn more.



