The AI security balancing act: From risk to innovation

A manufacturing CISO's guide to mastering the risk and potential of AI with insights based on NTT DATA's 2025 Global GenAI Report*

* Data points are based on responses from all manufacturing and automotive respondents, unless indicated otherwise. CISO statistics are based on manufacturing and automotive respondents who hold those titles, unless indicated otherwise.

Soaring investment in AI is already transforming industries and affecting the way we work and live

The increasing adoption of AI goes hand in hand with new and evolving cyberthreats

CISOs acknowledge the need for a modern, integrated cybersecurity posture

But how do CISOs help their organizations tap into the potential of AI while also protecting their digital assets from the risks?

We call this the AI security balancing act.

1. Is your cybersecurity strategy ready for the AI era?

While AI exposes businesses to new security risks, it also provides innovative tools and advanced capabilities to combat both traditional and evolving AI-driven cyberattacks.

GenAI has the potential to transform manufacturing

96%

of manufacturers say that GenAI is driving a new level of innovation in their organizations.

Over 1 in 3

evidence improved security as a direct result of GenAI deployments.

But progress comes with new security risks

88%

are highly concerned about the security risks associated with GenAI deployments.

Yet, only 43%

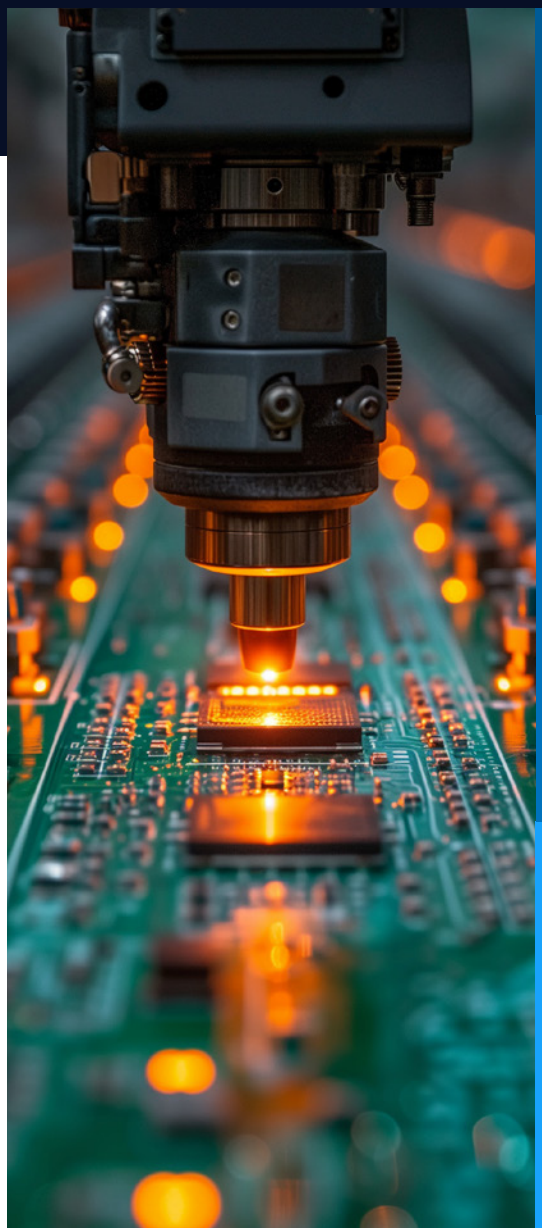
strongly agree that their current cybersecurity controls are effective in protecting current GenAI applications.

2. Understanding AI-related risks

The rapid integration of AI technologies expands attack surfaces and introduces sophisticated threats, making cybersecurity a critical business imperative.

Common types of AI attacks

- Adversarial attacks
- Data poisoning
- Algorithmic bias



Many manufacturers have only just started grappling with AI-related data management; however, efforts are intensifying.

Agentic AI will add a new dynamic and much value, but if it's not guided by well-defined data governance and privacy polices, implementation poses significant risks.

82% of manufacturers say that unclear government regulation on AI hinders innovation and investment in GenAI.

3. AI and security: CISOs must balance opportunity and risk

There is a notable disconnect between the strategic goals of the C-suite and the operational hurdles that CISOs face when striving to responsibly maintain security, privacy and compliance in AI deployments.

Strongest sentiment about Gen AI

100%

of CISOs in manufacturing (and 97% of CISOs across industries) claim to be principal decision-makers when it comes to GenAI.

Just 27%

of CISOs in manufacturing (and 33% of CISOs across industries) strongly agree that GenAI security risks are adequately understood and managed within their organizations.

The CISO challenge is compounded by aging, absent or unintegrated infrastructure

Top 2

challenges facing manufacturers in the next 2 years

1

Infrastructure complexity (such as modernization, performance/integration and lifecycle management)

2

Assessing complementary technologies (such as edge, IoT, 5G and GPUs)

92%

of manufacturers say that legacy infrastructure is holding back their GenAI progress.

Only 46%

strongly agree that their IoT devices generate sufficient volumes of data to support the development of robust GenAI models.

4. How CISOs in manufacturing can manage AI-related risks

Co-innovation and an end-to-end GenAI service offering are CISOs' top-ranked factors for deployment and assessing GenAI partners.

Key areas for managing AI risks with a multilayered approach

Improve observability

- Reimagine observability for AI.
- Maintain an inventory of AI assets and log new models.
- Upgrade your security operations center.

Develop an AI security policy

- Develop an AI security policy framework that outlines procedures for mitigating AI-related risks and sets out AI implementation methods.

Embed security by design

- Focus on data protection and privacy.
- Implement model validation and testing.
- Facilitate integration and compatibility.

Ensure continuous monitoring and threat detection

- Detect and respond to threats in real time.
- Maintain an incident-response plan.

Maintain risk management and compliance

- Conduct regular risk assessments.
- Understand the regulatory landscape.

Encourage collaboration and education

- Foster collaboration between security teams and AI developers.
- Educate employees about AI risks and best practices.
- Work with a trusted cybersecurity partner.

An AI-led, platform-first approach to cybersecurity will mitigate threats and turn cybersecurity into a strategic advantage that gives your organization a competitive edge.

NTT DATA empowers manufacturers to innovate safely and secure their business growth through AI-driven solutions.

Learn more about how we can help

Get the full report

Visit nttdata.com to learn more.

NTT DATA