Realizing value from AI and the evolving cyber threat landscape



US Japanese Practice | October 2026

Executive summary

The rapid evolution of generative AI presents unprecedented opportunities and significant security challenges. Many organizations struggle to realize tangible business returns due to the lack of a cohesive strategy and failure to achieve enterprise-wide deployment. Concurrently, the rise of Frontier AI is accelerating the cyber threat landscape, requiring organizations to transition from manual defenses to automated, AI-driven security processes. This article discusses common challenges faced by Japanese companies.

1 The generative AI evolution

The evolution of generative AI has been advancing at a tremendous pace since models were first made publicly available a few years ago. However, many may not have a tangible sense of the scale of this progress.

For instance, third-party benchmark evaluations of autonomous task execution indicate an extraordinary leap in capability. While early 2022-era large language models could only successfully complete simple tasks equivalent to under a minute of human effort, modern 2026-era reasoning-class models are capable of autonomously executing highly complex, multi-step tasks that would require approximately 16 hours of human labor. Furthermore, with performance observed to be doubling approximately every four months, projections suggest that within a few years, generative AI systems may be capable of performing tasks that would take a human a full month to complete. Considering that AI is now poised to handle these workflows, the technology has clearly undergone a massive evolution compared to the simple Q&A models of the past. While we cannot say AI will be capable of doing everything, it will undoubtedly take on a significant portion of our daily work.

Although AI is being introduced in many companies, it is becoming clear that few are realizing tangible business returns from their AI utilization. While there are many potential reasons, this article will focus on two common points observed through AI engagements and discussions with Japanese companies.

2 Key challenges in realizing AI value

2.1 Lack of a cohesive AI strategy

To realize business benefits from AI, it is important to formulate an AI strategy that is intrinsically linked to the overall business strategy. This approach must clarify which areas of the business can generate returns through AI

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

implementation. While there is a phase where allowing employees to voluntarily use AI or build AI agents is necessary, this approach alone often falls short of producing measurable business returns. The AI strategy should also explicitly define how returns will be measured and, of course, it is critical to periodically evaluate ROI and adjust the direction as needed.

2.2 Failure to achieve enterprise-wide deployment

A 2025 MIT study on task-specific LLMs reported that only 5 percent of companies had achieved full, enterprise-wide deployment[1]. This is often because initiatives that start with a "pilot implementation for now" mindset neglect other critical areas of transformation, such as data, people, governance, and business processes. It should be noted that the "pilot for now" itself is not the problem, but rather the lack of attention paid to these other crucial aspects. Here, we will focus on three of these: data, people, and governance.

- **Data readiness:** As the foundation for any AI implementation, preparing data is extremely important. Because pilots are often confined to a specific department, data readiness across departments becomes a critical factor when expanding enterprise-wide. At the same time, making the complete overhaul of all company data a prerequisite for AI adoption will stall progress. A degree of ingenuity is required, such as focusing on preparing only the data necessary for a particular AI implementation.
- **Human capital and people:** Introducing AI does not make the workforce redundant. On the contrary, it creates the need for people to work with AI, making investment in human capital more important than ever. Training is the most obvious component, but there are several other key points:
  - **Fostering psychological safety:** AI implementation involves trial and error, so it is necessary to cultivate an environment of psychological safety where failure is accepted.
  - **Revising evaluation systems:** For instance, an employee who can complete a specific task in a short amount of time using AI should arguably be evaluated more highly than an employee who takes much longer to complete the same task without it. Therefore, a shift toward output-based performance evaluations should be considered.
- **Governance:** Many users do not trust the results produced by AI, and they feel that outputs created by others using AI are even less reliable. It is important to visualize and share the reliability of AI-generated answers and materials. KPMG offers frameworks that can help make the trustworthiness of AI outputs transparent.

3 Cyberattacks using Frontier AI

Up to this point, we have briefly described the elements necessary to build AI that delivers direct business returns. However, AI also has a negative side, one aspect of which is the use of Frontier AI in cyberattacks. Here, we will briefly introduce why Frontier AI is poised to energize cyberattacks and what the future of the cyber world may hold.

Because the offensive cyber capabilities of Frontier AI are covered in newspapers and other sources, details will be omitted here. However, it is anticipated that the time from vulnerability discovery to attack execution will shorten rapidly, enabling threat actors to complete an attack in less than 24 hours. In contrast, many organizations take around 60 days to apply corrective patches, and operational technology (OT) systems in environments like factories can take an average of 18 months. This creates a scenario where defenders require anywhere from 60 days to 18

[1] Source: MIT Project NANDA, *The GenAI Divide: State of AI in Business 2025*, July 2025

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

months to remediate vulnerability, while attackers can identify and exploit it within 24 hours—a severe asymmetry that underscores the urgency of automated defense.

Table: Vulnerability response timelines

Role	Action	Timeline
Threat actors	Vulnerability discovery to attack	< 24 hours
Standard organizations	Applying corrective patches	~60 days
Operational technology (OT)	Patching in factory environments	~18 months

Source: KPMG analysis based on observed threat intelligence trends regarding AI-driven attack speeds, as well as industry averages for enterprise vulnerability remediation and operational technology (OT) maintenance cycles (2026).

Furthermore, we are beginning to see the parallelization of attacks using AI agents. A defense that relies solely on humans will likely not withstand an attack that exploits multiple vulnerabilities simultaneously. While only models with suppressed cyberattack capabilities have been released so far, high-performance, low-cost open-source models are emerging. It is anticipated that the day is not far off when malicious groups or individuals will have access to models without such restrictions.

4 Automating defensive processes

To counter such attacks, organizations may wish to automate their defensive processes. However, telling an organization to simply "start automating with a defensive AI agent tomorrow" is not a feasible request. The automation of defense processes has several crucial prerequisites (only a portion is listed here due to space constraints):

- **Centralized management of attackable IT assets:** All assets such as IT infrastructure, identities, internet-facing services, and their dependencies must be centrally identified and managed. It is impossible to apply multilayered defenses to assets that are not centrally managed and visible.
- **Operationalizing rapid patch application for critical assets:** Because applying patches can address vulnerabilities, it is necessary to begin operating a process to apply them quickly, for instance, within 60 minutes of their release.
- **Automation of containment and mitigation measures:** There is a significant possibility of being attacked before a patch is released. Therefore, it is necessary to prepare a process to automatically isolate compromised IT assets. However, as various stakeholders are currently involved in decisions to isolate IT assets, and many services and business processes cannot be easily stopped, organizations must start by visualizing the isolation and segmentation process for each IT asset to prepare for automation with AI agents.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

5 Conclusion

AI is a tool. It can be a highly effective tool for business transformation, customer satisfaction improvement, and business model innovation. It can be used for both cyber offense and defense. At the same time, the option to not use AI is progressively disappearing. To maintain a competitive edge and resilient security posture, organizations should strategically integrate AI into both the offensive and defensive aspects of their business.

Contact us



Nobuhiro Tamura
Senior Director, Advisory
KPMG LLP
ntamura1@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

About this Translation: This document is an English translation of an original article prepared in Japanese. Artificial intelligence (AI) tools were used to prepare this English translation. In the event of any discrepancy, inconsistency, or ambiguity between the English translation and the original Japanese text, the Japanese original shall prevail. The original Japanese version is the authoritative source.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.