January 2026

Japan Newsletter

NÍSHLÍS
10 Years | GLOBAL LEGAL MARKETING

Introduction

In this second edition of our Japan newsletter, we focus squarely on the domestic developments reshaping Japan's political and regulatory landscape, and what they signal for the country's direction in the years ahead.

Japan's new Prime Minister has moved quickly to articulate a firmer economic-security and national-defense posture, reflecting mounting regional pressures and long-standing structural vulnerabilities. Defense spending is accelerating toward unprecedented levels, with direct implications for Japan's defense, aerospace, cyber, and advanced manufacturing industries. These shifts mark one of the most significant evolutions in Japan's post-war security policy and are already influencing industrial strategy, procurement, and international collaboration.

Cybersecurity stands at the heart of this transformation. Japan's enactment of the Active Cyber Defense framework represents a decisive break from a purely reactive model, embedding proactive threat detection, closer public-private coordination, and stronger institutional leadership into national policy. Alongside this, Japan continues to refine an innovation-first approach to AI governance and critical-infrastructure protection, balancing security, economic resilience, and technological progress.

This edition is informed by the insights of leading Japanese experts working at the intersection of policy, academia, and industry. We are honored to feature perspectives from Dr. Kenzo Fujisue, Professor at MIT Sloan and former Japanese State Minister for Internal Affairs and Communications, who played a central role in shaping Japan's national cyber framework, and we extend our thanks and gratitude to Eddy Almand, Founder and CEO of Almata, for his on-the-ground perspective on Japan's evolving cyber threat environment. Their insights bring depth and clarity to a pivotal moment for Japan.

Editor
Lee Saunders

Table of Contents

Japan's Shift to Active Cyber Defense

Isaku (Isaac) Uchiyama
VP Asia Pacific / Head of Tokyo Office
Nishlis Global Legal Marketing

What Global General Counsel Should Know — and How Nishlis Japan Supports Strategic Execution

Japan has long been viewed as a "high-trust" market: strong institutions, resilient infrastructure, and generally predictable regulation. But the threat environment around Japanese operations has changed. Ransomware, supply-chain compromises, and state-linked intrusion campaigns increasingly target Japan's critical infrastructure and globally connected private sector. Against that backdrop, Japan has begun a decisive shift from a historically reactive cyber posture toward "active cyber defense" - a shift global general counsel should track closely as it reshapes incident obligations, regulator expectations, and cross-border risk.

In 2025, Japan moved to enable a more proactive model for preventing severe cyberattacks, including deeper coordination between government and industry and faster disruption of malicious activity. Just as importantly, Japan has been strengthening the institutional "center" of cybersecurity inside government -aimed at clearer coordination, more consistent policy, and more structured engagement with the private sector. For multinational enterprises, the takeaway is not simply "new rules," but a new operating reality: faster timelines, more touchpoints, and higher expectations around preparedness.

Why China–Japan dynamics now matter for cyber risk

Cybersecurity in Japan is increasingly intertwined with national security. Japan's regional security environment – particularly the rise in strategic friction with China—has sharpened attention on critical infrastructure resilience, supply-chain integrity, and the risk of state-linked espionage against sensitive sectors (telecommunications, advanced manufacturing, aerospace, semiconductors, defense-adjacent technologies, academia, and government-connected bodies). Even when an incident is criminal on its face, many organizations now assume a higher likelihood of state interest somewhere in the chain—through tooling, infrastructure, proxies, or target selection. That shifts the legal and governance burden: threat modeling becomes more geopolitical, and incident decisions (communications, regulator engagement, evidence strategy, data handling) must be made with greater speed and discipline.

What this means in practice for in-house counsel

Three themes stand out.

First, expect more structured public-private touchpoints—especially around critical infrastructure and strategic

supply chains. Even if your organization is not formally designated as critical infrastructure, you may feel spillovers through customers, suppliers, and sectoral standards. Contract terms, incident reporting workflows, vendor management, and evidence readiness become more important—and more scrutinized.

Second, "active" defense puts greater emphasis on network-level telemetry and faster disruption—with privacy and oversight guardrails. This raises practical questions for global organizations: what data is collected, where it is processed, how it is shared across borders, and how it intersects with privacy compliance and employment/HR considerations. It also raises strategic questions: when authorities can act faster, the organization must be prepared to respond faster.

Third, the reforms change the tempo of incidents. When the objective is to detect and disrupt campaigns earlier, the window for decisions compresses dramatically: privilege strategy, notification thresholds, regulator engagement, communications posture, and board updates may need to happen in the first 24–72 hours. The most cost-effective mitigation is governance: a rehearsed escalation pathway spanning legal, privacy, infosec, comms, HR, and business leadership; clear authority and decision rights; and a practiced, privilege-aware playbook.

Where Nishlis Japan fits: trusted access + faster execution

In this environment, the differentiator is not just knowing the law—it is having trusted access to the right Japan expertise early, and the ability to convert that expertise into defensible decisions and coordinated action.

Nishlis Japan exists to build bridges between global legal leadership with experts across Japan, including in its cybersecurity ecosystem. provides trusted access to Japan-specialist counsel.

Global General Counsel and in-house legal teams

We help you translate Japan's evolving cyber posture into actionable readiness and response. Typical support includes:

- **Right-counsel matching in Japan:** introductions to Japanese law firms with proven cyber, privacy, investigations, and regulatory capabilities—aligned to your industry and risk profile.
- **On-the-ground strategic context:** we can connect you to Japan-based strategic advisors who understand how decisions land operationally and reputationally in Japan, including our featured experts in this newsletter, **Dr. Kenzo Fujisue** and **Eddy Almand.**

- **Incident-speed execution support:** help aligning legal, privacy, infosec,

comms, HR, and business leadership on escalation paths, decision rights, and privilege-aware response.

- **Partner and solution pathway (through our connections with One Line Group (OLG), when relevant:** support in evaluating cyber/ AI partners and technologies connected to your Japan footprint—especially where supply-chain assurance and implementation speed are key .

International law firms supporting clients with Japan exposure

We help international firms deliver Japan capability to clients—without losing momentum or control of the relationship. Typical support includes:

- **A "Japan extension" for your client teams:** Nishlis coordinates introductions to suitable Japanese counsel and strategic operators, so you can deliver a coherent cross-border response.

- **Client-facing briefings you can offer immediately:** we can organize a structured briefing with Japan legal and strategic expertise, tailored to your client's sector, footprint, and risk posture.

- **Coordination across time zones and stakeholders:** we help reduce friction—ensuring the right people are in the room early, aligned on facts, priorities, and decision rights.
- **Commercial and implementation context (via our connections with OLG):** where clients need market-facing support alongside legal strategy—scoping, partner evaluation, and practical Japan entry/adoption pathways.

A simple way to think about it

Japan's cyber reforms—and the broader geopolitical context—are pushing cyber issues from "IT risk" into "board-level legal risk." Nishlis Japan helps global GCs and international firms respond with speed and clarity by connecting them to the right Japan expertise and ensuring that advice becomes execution.

If you would like to discuss Japan cyber specialist counsel introductions, or Japan on-the-ground strategic support, please contact **Isaac Uchiyama** at Isaac@nishlis.com

Why Japan Is Becoming a Strategic Cyber Hub in Asia

Dr. Kenzo Fujisue

We spoke with **Dr. Kenzo Fujisue,** who provided rare, first-hand insight at the intersection of Japanese cyber policy, government decision-making, and commercial execution. Dr. Fujisue combines academic leadership at MIT Sloan's Cybersecurity at MIT Sloan (CAMS) with nearly two decades shaping Japan's national cyber framework from inside government, including drafting the Cybersecurity Basic Act. He served for more than 18 years in Japan's House of Councillors (Senate), including as State Minister for Internal Affairs and Communications, and previously spent 13 years at the Ministry of Economy, Trade and Industry. He also serves as a Project Professor at Keio University.

Over the past three years, Japan has undergone a significant political and legislative transformation, driven by an urgent need to overcome structural vulnerabilities and assert its role as a strategic, high-trust partner in the Indo-Pacific. Landmark reforms such as the Economic Security Promotion Act (ESPA) and the planned implementation of Active Cyber Defense (ACD) illustrate this shift.

What are the strategic drivers for Japan's market appeal in Cyber?

Japan's recalibration as a regional cyber hub is driven by domestic digital mandates and intensified by external geopolitical imperatives. The establishment of the Digital Agency in 2021 marked a turning point, accelerating demand for advanced security architectures across cloud, IoT, and operational-technology (OT) environments. According to IMARC Group, the Japanese cybersecurity market was valued at USD 18 billion in 2024 and is projected to grow at a CAGR of 10.3%, reaching USD 43.3 billion by 2033.

Complementing this domestic growth is Japan's strategic role as a principal actor in harmonizing international cyber norms. Through active participation in G7, QUAD initiatives, and the U.S.–Japan alliance, Japan cultivates a regulated "high-trust environment." This posture is essential for foreign firms engaging in sensitive technological collaboration, effectively positioning Japan not merely as a market, but as a secure regional anchor for Western partners expanding into Asia.

What are the market catalysts for its appeal?

Concurrently, Japan's attractiveness is defined by critical structural challenges that act as a persistent demand-pull for sophisticated global expertise. The nation suffers from a chronic and severe

shortage of cybersecurity professionals, a deficiency that transforms the talent deficit into a prime opportunity for foreign firms offering AI-driven automated defense tools. According to a 2025 report by Japan's Ministry of Economy, Trade and Industry (METI), the country faces a shortage of approximately 110,000 cybersecurity professionals — a gap that significantly exceeds current domestic capacity and underscores the urgent demand for external expertise. In this context, advanced technology acts as a vital "force multiplier" to supplement a limited human workforce.

Furthermore, the architectural reality of the Japanese economy—where Small and Mid-sized Enterprises (SMEs) constitute over 99% of businesses and employ 70% of the workforce—creates an interconnected yet defensively fragmented supply chain.

How has Japan's cyber governance framework evolved?

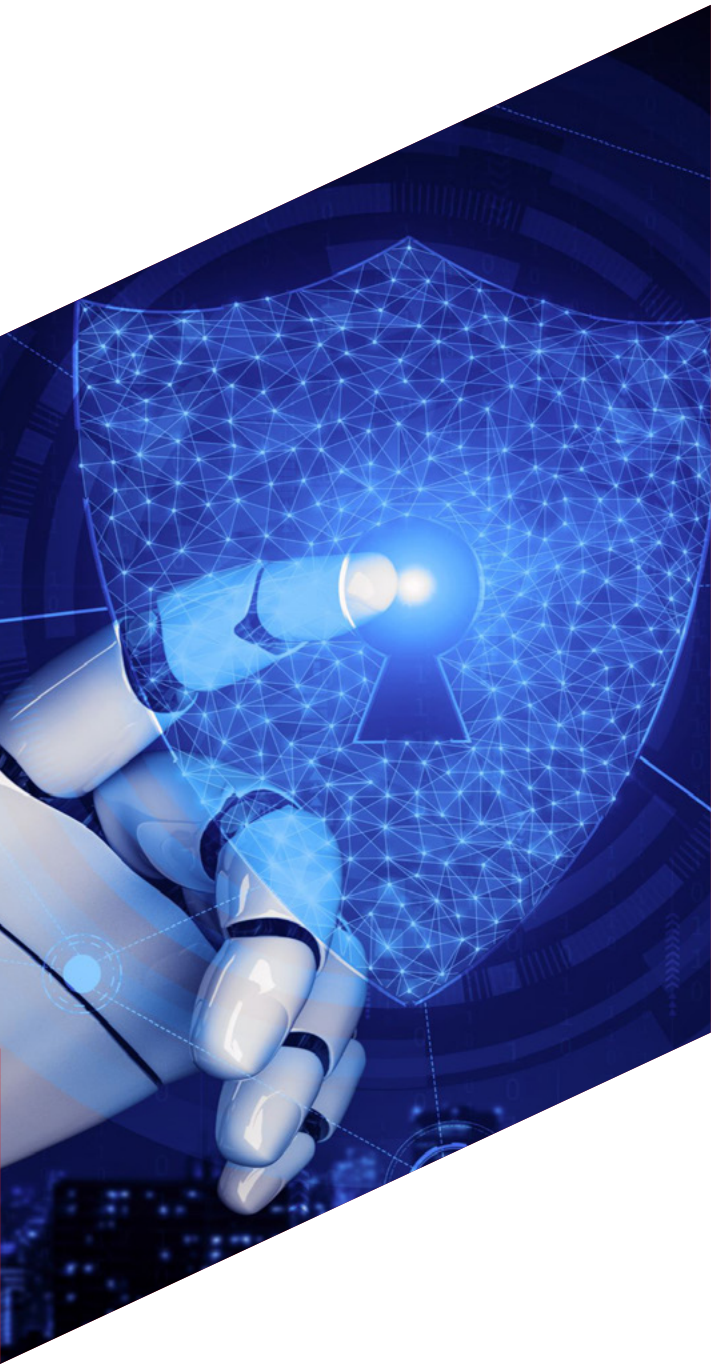
Current Japanese cyber policy represents a fundamental shift away from administrative fragmentation toward a centralized, industry-aligned command structure. This momentum is sustained by a robust political mandate for regulatory overhaul. The institutionalization of reforms such as Active Cyber Defense (ACD) is driven by the commitment of leaders like Sanae Takaichi, whose expertise ensures high-level political backing for proactive defense.
This centralization of execution is increasingly expert-led, evidenced by the strategic appointment of industry and trade-focused professionals. The elevation of Yoichi Iida as the Cabinet Cyber Official (Vice-Minister Class) and the appointment of Professor Ikuo Misumi to the Digital Agency—both distinguished alumni of the Ministry of Economy, Trade and Industry (METI)—reflect a national commitment to pragmatism. By adopting an "economically-minded" approach, the Japanese government is moving beyond bureaucratic formality to ensure that cyber defense is executed with the speed and industrial focus required in the modern geopolitical era.

How and why has Japan adopted an innovation-first approach to AI and cybersecurity?

Japan's regulatory and strategic approach to AI-driven cyber threats represents a paradigm shift—prioritizing innovation as a mandatory compensatory mechanism for its acute labor shortage. Unlike the compliance-heavy mandates of the European Union, Japan's "innovation-first" model utilizes AI as a fundamental force multiplier. Japan's deviation from Western regulatory models does not merely reflect policy differences — it creates a competitive entry window where foreign firms can scale AI-security deployments faster and with fewer compliance burdens.

What does this mean for global companies compared with Western regulatory regimes?

This pragmatic agility presents a sharp contrast to the regulatory philosophies of the European Union and the United States. The European approach, exemplified by the EU AI Act, is built upon a comprehensive, risk-based regulatory framework focused on "rights-centered" compliance. By prioritizing societal risk mitigation ahead of deployment, the EU creates a high-hurdle environment that some industry critics argue may impede the pace of innovation. Conversely, the United States relies on a primarily market-driven model utilizing voluntary standards like the NIST Cybersecurity Framework.



Japan occupies a unique middle ground: it maintains an open market with an acute, defense-critical need for AI innovation. By framing AI as a tool for efficiency and social good, Japan has cultivated an "innovation-first" ecosystem. This regulatory environment avoids technology-mandated compliance checks in favor of adapting existing laws, such as the Act on the Protection of Personal Information (APPI), to address concrete risks without stifling growth.

Where Can Global Firms Plug into Japan's Cyber Defense Gap?

Japan's urgent defensive needs create significant direct opportunities for Western firms to bridge the structural gap. Immense demand exists for scalable, AI-driven defense solutions—specifically "AI-as-a-Service" tools that provide automated detection and response capabilities for SMBs and municipalities currently unable to afford traditional SOC operations. Furthermore, as Japan prioritizes future technologies such as post-quantum cryptography (PQC), collaboration in securing AI governance becomes paramount.

Global partners are invited to help build an "Asian model of trust." By assisting Japanese firms in refining

ethical frameworks that bridge domestic principles with international standards like GDPR, foreign organizations can position themselves as key enablers of Japan's national digital resilience. Japan is not merely an open market; it is an ideal testbed and launchpad for the next generation of intelligent cybersecurity.

What does Japan's move to Active Cyber Defense mean in practical terms for how cyber threats are handled and how companies must operate?

Japan's Active Cyber Defense (ACD) legislation represents a foundational, political-led transformation of the nation's security posture. Moving beyond a traditionally reactive stance, the framework established under the 2022 National Security Strategy (NSS) aims to deter, detect, and neutralize threats in the early stages of an attack. This law fundamentally alters the rules of engagement for critical infrastructure operators, data handling, and public-private cooperation within Japan. By institutionalizing this shift, the Japanese government has signaled a new era where intelligence-led defense becomes mandatory for national resilience.

The momentum behind ACD is institutionalized through centralized political leadership and expanded statutory powers. The momentum is driven by the political commitment of leaders like Sanae Takaichi. This leadership led to the creation of the Cabinet Cyber Official (Vice-Minister Class), a command structure recently filled by former METI official Yoichi Iida to institutionalize centralized coordination for ACD. To establish robust early warning capabilities, the law grants the government statutory authority to intercept and collect metadata from foreign internet traffic traversing domestic infrastructure. Beyond monitoring, ACD authorizes the government to implement measures to monitor, penetrate, and neutralize an attacker's infrastructure to suppress future attacks. Specialists from the police and military are authorized to carry out these functions, occasionally without prior judicial approval due to time constraints.

The institutionalization of ACD mandates that global partners and foreign providers adjust their operations to meet Japan's rigorous security environment. Critical infrastructure operators in sectors such as finance, energy, and transportation must now comply with mandatory requirements for reporting cyber incidents to the government. This legal obligation necessitates that foreign firms implement clear, rehearsed playbooks and decision frameworks for rapid disclosure. Providers of critical systems are further expected to demonstrate high-assurance security controls and rigorous Zero Trust principles to protect access. Japan prioritizes collaborations that deliver solutions adhering to international standards such as NIST or ISO, favoring partners that align with its enhanced national security posture.

Why has collaboration between Japan and Western partners become a strategic necessity?

Collaboration between Japanese companies and their U.S./European counterparts has transcended traditional commercial exchange, evolving into deep, government-backed strategic partnerships. These synergies are concentrated in sectors where Japan prioritizes strategic independence and the systematic overhaul of structural security vulnerabilities. This momentum, sustained by robust political leadership from figures such as Sanae Takaichi and METI alumni Yoichi Iida and Ikuo Misumi, positions cyber resilience as a national imperative that requires integrating advanced foreign expertise.

The protection of Japan's manufacturing ecosystem is paramount. According to the National Police Agency (NPA), the manufacturing sector accounted for 31% of domestic ransomware incidents in 2023 , making it the most targeted industry in the nation. This structural vulnerability, exacerbated by intricate supply chain interdependencies, necessitates vital Western expertise in securing Operational Technology (OT) and the broader industrial base. Collaborations now emphasize proactive methodologies such as Software Bill of Materials (SBOM) analysis and Zero Trust Architecture (ZTA), which are essential for securing critical infrastructure and high-value manufacturing hubs.

As Japan modernizes its financial infrastructure, strong collaboration opportunities exist in Fintech and RegTech (Regulatory Technology). There is an escalating demand for advanced, AI-leveraged AML/CTF and fraud detection tools to manage the fragmented and complex data security requirements inherent in global financial crime prevention. Ultimately, these multisectoral collaborations—from the Global Combat Air Programme (GCAP) to secure payment systems—are driving Japan's path toward national digital resilience. By integrating Western innovation with Japanese industrial stability, these partnerships are co-creating a new "Asian model of trust."

Why Japan is Asia's Gateway

Eddy Almand
Founder and CEO of Almata

ALMATA

Eddy Almand, Founder and CEO of Almata, shared his insights on Japan's role as a regional cyber hub, its Cyber Defense Law, and much more. Almata is a Japan-based cybersecurity company dedicated to delivering scalable, automated, and intelligence-driven security solutions for organizations operating in an increasingly complex digital and geopolitical environment.

What recent developments make Japan a more attractive entry point into Asia for European and U.S. companies looking to strengthen their cyber strategy?

In the past few years, Japan has quietly become one of the most attractive Asia-entry markets for European and U.S. companies that take cybersecurity seriously. Three developments, in particular, stand out from my perspective:

1. **Economic security and critical-infrastructure reforms.**
   The Economic Security Promotion Act and the new framework for "Specified Essential Infrastructure Services" have significantly raised expectations around cyber resilience, vendor transparency, and business continuity across sectors such as energy, telecommunications, finance, and logistics. For foreign firms, this creates a highly regulated yet predictable environment that increasingly resembles U.S. and EU standards. Although Japan is relatively new to implementing these reforms, it is drawing heavily on Western lessons learned, which makes the transition smoother for companies already operating under mature governance models.

2. **Sector-specific cyber/physical standards.**
   METI and related agencies have issued detailed cybersecurity guidelines for factory systems, power-control systems, semiconductors, and broader OT/ICS environments, all mapped to frameworks such as NIST CSF and Japan's own Cyber/Physical Security Framework (CPSF). For U.S. and European providers of OT security, monitoring, and managed services, this creates a clear roadmap for localization. At the same time, there is a well-known skills and knowledge gap in Japan around OT/ICS cybersecurity, making foreign expertise especially valuable.

3. **Shift to active cyber defense and deeper alliances.**
   Japan's new Active Cyber Defense Law

marks a decisive shift away from a purely reactive posture and aligns the country more closely with U.S. and UK approaches to operational cyber defense. For Western vendors, this translates into:

- growing demand for high-end threat intelligence,
- increased appetite for advanced detection and response capabilities, and
- a policy environment that is more closely synchronized with allied democracies.

Taken together with Japan's strong rule of law, IP protection, and political stability, the country is emerging as a trusted cyber hub and a credible regional base for operations into the broader Indo-Pacific, including markets where data hosting or operational presence may carry higher risk.

The common theme across all of this is that Japan is rapidly adopting global best practices, yet the domestic talent pool and institutional knowledge have not fully caught up. While there are excellent specialists in country, they remain the exception. Simply introducing products into the market is rarely enough; the real opportunity lies in helping Japanese organizations strategically apply the right security solutions and services to reduce their exposure to accelerating cyber risks.

How is Japan approaching AI-driven cyber threats differently from the U.S. and Europe, and where does this create opportunities for foreign firms?

Japan's approach to AI and cyber risk is notably more guideline-driven and consensus-based than the hard-law regulatory model emerging in the EU. Several themes stand out from what I am seeing on the ground:

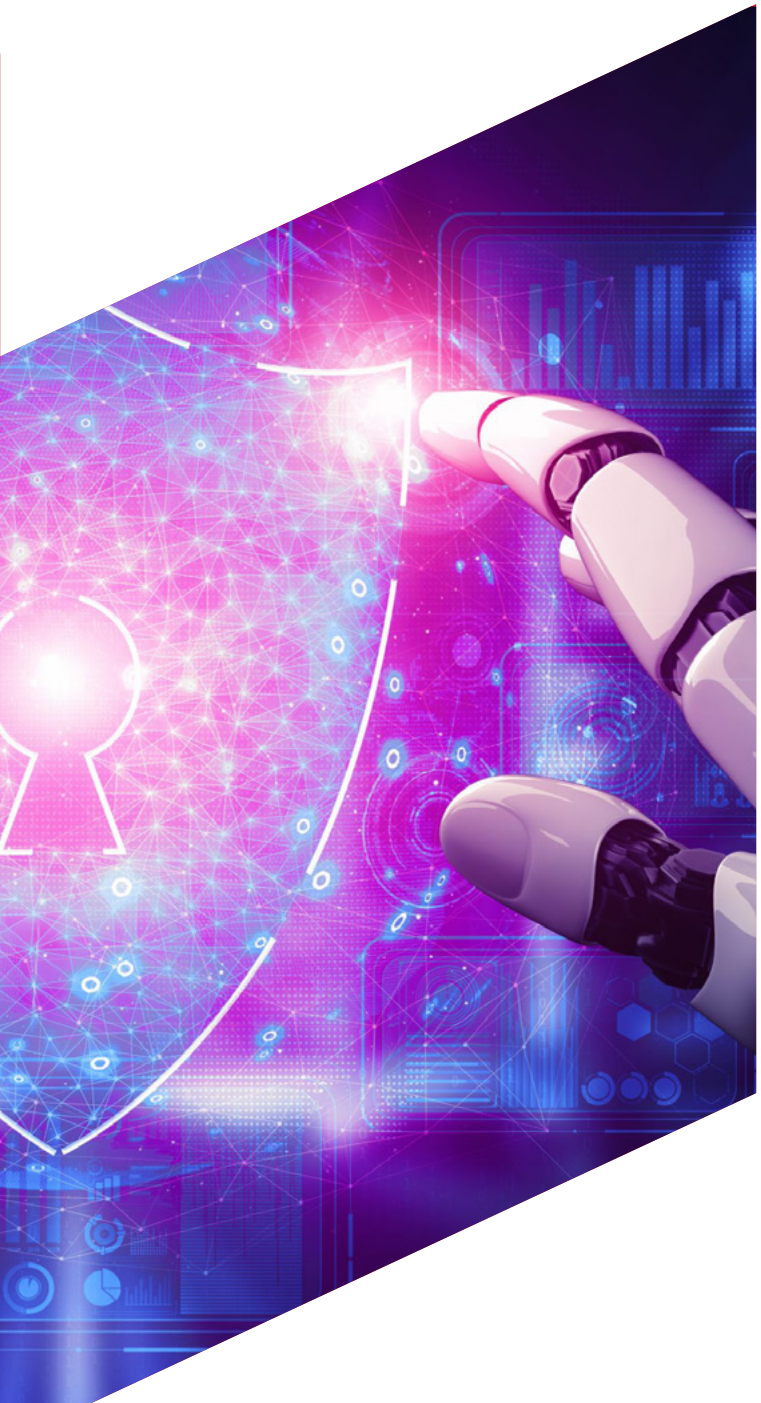
1. **Soft law first, regulation later.**
   Japan has issued AI Guidelines for Business and broader AI-governance guidance that emphasize a risk-based approach, executive accountability, and integration of AI oversight into overall corporate risk management. Although non-binding, these guidelines function as "soft law" because they are increasingly embedded in procurement requirements and contractual expectations.

2. **AI safety and cybersecurity are converging.**
   The AI Safety Institute (AISI) and related initiatives directly link AI safety to cybersecurity protecting models and data, addressing prompt-based attacks, and mitigating disinformation risks. In contrast to the U.S., where adoption often precedes governance, Japan is attempting to "bake in" safety and security considerations from the beginning.

3. **Public-sector procurement will shape market behavior.**

New guidance on government use of generative AI references existing cybersecurity standards for public agencies. Any AI solution entering this domain must therefore meet both AI-governance and cybersecurity obligations simultaneously.

4. Products alone are insufficient—Japan expects service capability. A critical point for foreign entrants is that simply having a strong product is rarely enough for the Japanese market. Organizations expect a service layer that contextualizes, localizes, and operationalizes the technology. This often takes one of two effective forms:



- Partnering with a domestic service provider that can deliver managed support, localization, and ongoing governance in Japanese; or

- Building your own service package tailored to Japan, including local-language documentation, policy templates, advisory support, and integration with Japan's AI and cybersecurity frameworks.

In practice, the companies that succeed in Japan are not those that "sell a product," but those that demonstrate how the product becomes a solution within Japan's regulatory, cultural, and operational context.

Where this creates opportunities for foreign firms:

- Security tools that protect the AI pipeline such as models, training data, inference APIs while mapping cleanly to Japan's AI governance frameworks.

- Integrated services that blend AI red-teaming, disinformation resilience, and traditional cyber defense for government, critical infrastructure, and major manufacturers.

- Firms able to translate U.S./EU AI-security best practice into Japanese-language, regulator-friendly deliverables, such as

governance policies, audit trails, and assurance documentation.

- Solution-plus-service models, where foreign technology is paired with local advisory, monitoring, or integration services to meet Japan's expectation for long-term support and operational partnership.

For companies entering the market, alignment with Japan's AI guidelines, its established cybersecurity standards, and its expectation of service-driven value will be the key differentiators.

What should global companies understand about Japan's new Active Cyber Defense law and how it may affect operations or partnerships in the country?

Global companies need to understand that Japan's new Active Cyber Defense Law is not just a government issue; it will change expectations for operators, vendors, and partners in and around Japan.

At a high level, the law:

- It was enacted in May 2025 and will become operational around 2027.
- Allows designated authorities (police, Self-Defense Forces, etc.) to:
- monitor and analyze cross-border internet traffic involving foreign IPs, and
- neutralize foreign servers being used as staging points for cyberattacks against Japan, for example takedowns and sinkholing.
- Explicitly focuses on foreign-related traffic, with stronger safeguards for domestic communications, reflecting constitutional and privacy constraints.
- Tightens incident reporting obligations for critical infrastructure and other specified operators, including those under the broader economic security regime.
- For multinational companies and partners, the practical implications are:

1. **More structured cooperation with Japanese authorities.**
   - If you operate critical infrastructure or provide key cyber services, you should expect formalized information-sharing, incident reporting and possibly participation in joint threat-disruption operations.
2. **Greater scrutiny of your logging and data-handling practices.**
   - Authorities may need metadata and logs to identify hostile infrastructure. You will need clear governance around what can be shared, under what legal basis, and how that interacts with GDPR and other cross-border data regimes.
3. **Contractual and risk-allocation questions.**
   - If Japanese authorities act against malicious servers hosted in your cloud environment or supply chain, where does liability sit? Your GC and security leadership should

be reviewing contracts, SLAs and incident-response playbooks with this law in mind.

4. **Reputational and geopolitical risk management.**
   - "Hack-back" is politically sensitive. Even under a strict legal regime, mistakes in attribution can have diplomatic consequences. Companies supporting Active Cyber Defense operations must be careful about governance, documentation and boards' understanding of the risk.

In short, treat Japan's ACD law as a strategic change in the operating environment, not just a technical detail.

As Japan raises the bar on critical-infrastructure and supply-chain security, what are the key implications for foreign organizations working with Japanese partners?

Japan is raising the bar on critical-infrastructure cybersecurity in three principal ways that foreign organizations will clearly feel:

1. **Designation and oversight of "essential infrastructure."**
   Under the economic security framework, key sectors are now formally designated and subject to enhanced oversight. This includes more rigorous risk assessments, reporting obligations, and elevated security expectations across the full lifecycle of systems and software.

2. **Deepening cyber/physical and OT standards.**
   METI's Cyber/Physical Security Framework, along with sector-specific guidelines for factory systems, power systems, and semiconductor facilities, provides highly prescriptive requirements for asset management, network segmentation, monitoring, incident response, and physical security aligned closely with NIST CSF 2.0.

3. **Software supply-chain and SBOM requirements.**
   Japan is transitioning toward systematic SBOM utilization and stricter software supply-chain controls, especially for vendors serving critical infrastructure and public-sector environments.

For foreign organizations working with Japanese partners, these developments translate into:

- More intensive due-diligence requirements regarding your own suppliers, development processes, and updating mechanisms.
- Mandatory alignment with recognized security frameworks (NIST CSF, ISO/IEC 27001, CPSF, etc.) and an expectation to demonstrate implementation, not merely reference policies.

- A strong preference for transparent and explainable controls, including clarity on data residency, subcontractor involvement, and vulnerability management practices.

- The necessity of providing Japanese-

language documentation and local support, as English-only materials will not satisfy regulators or internal risk committees.

If you can articulate a coherent and well-evidenced approach to SBOM usage, OT security, and vendor-risk management that maps cleanly to Japan's guidelines, you make life significantly easier for your Japanese counterparts and that becomes a meaningful competitive advantage.

It is also worth noting that Japan has historically approached compliance in a largely binary, checklist-driven manner where controls are marked as pass or fail, rather than evaluated through a holistic, risk-based lens. Bringing the ability to connect security risk analysis to those checklist controls and to explain the rationale clearly adds substantial value in this market.

From your regional experience, what are the biggest challenges General Counsels face today in managing cyber and geopolitical risk across Asia?

From a regional perspective, General Counsels in Asia are confronting a convergence of cyber, data, and geopolitical risk that is far more complex than what many boards have traditionally encountered.

The principal challenges include:

1. **Regulatory fragmentation.**
   Each jurisdiction, Japan, Korea, Taiwan, the ASEAN states, India, maintains its own combination of cybersecurity, data-protection, and sector-specific regulations. Harmonizing a global policy framework with local compliance requirements across such diverse markets is exceptionally difficult and non-trivial.

2. **Economic security and "de-risking" pressures.**
   Japan's economic security laws, U.S. export controls, and EU supply-chain and data-sovereignty regulations intersect across the region. As a result, GCs must routinely address questions such as: Can we host this workload in this country? Is this vendor permissible? Does this transaction trigger export-control or national-security review?

3. **Third-party and supply-chain risk at scale.**
   A significant proportion of attacks in Asia originate through local service providers, distributors, and joint-venture partners. Legal teams must translate "zero-trust" principles into contracts, due-diligence mechanisms, and enforceable audit rights while preserving commercial relationships. In Japan in particular, where SMBs comprise more than 99% of all businesses and often lack adequate cyber resources, these smaller firms frequently become the weakest link and a gateway for adversaries seeking to disrupt larger organizations.

4. **Grey-zone and geopolitical pressure.**
   Geopolitical tension in the Indo-Pacific is heating up and it increasingly shapes

the operational, legal, and security posture of companies across Asia. General Counsels now contend with a risk environment where commercial activity, technology development, and national security are going to be more intertwined.

Several dynamics are driving this pressure:

- **State-aligned cyber activity targeting commercial entities.** Organizations may be targeted because of their strategic relevance, defense partnerships, critical-infrastructure roles, semiconductor or AI capabilities, or even their position in a supply chain linked to U.S. or Japanese national-security interests. Attacks may be designed not to steal money, but to collect intelligence, erode trust in systems, or shape decision-making during diplomatic friction.

- **Expansion of grey-zone behavior.** Grey-zone operations and actions intentionally kept below the threshold of armed conflict are becoming more frequent. These range from coordinated cyber intrusions and disinformation campaigns to economic coercion and lawfare. Companies can become pressure points in broader geopolitical disputes, even if they are not directly involved in defense or government work.

- **Technology as a strategic battleground.** Sectors such as AI/ML, autonomous systems, cloud infrastructure, and advanced manufacturing now sit at the center of regional competition. Firms in these domains face heightened scrutiny, targeted intrusions, and complex export-control landscapes. GCs must ensure compliance with overlapping regimes while maintaining operational continuity and protecting sensitive IP.

- **Jurisdictional risk.** Decisions about where data is hosted, where staff are located, and where infrastructure is deployed now carry geopolitical implications. Hosting in the wrong jurisdiction or relying on a vendor with exposure to a high-risk state can introduce both cyber intrusion risk and regulatory exposure under U.S., EU, and Japanese national-security frameworks.

- **Human and operational security.** Beyond network security, companies may face threats to personnel or facilities, particularly where they operate near politically sensitive areas or engage with defense-related clients. GCs must prepare for scenarios involving staff safety, travel risk, and government requests for information or cooperation.

- **Public narrative and reputational risk.** Companies may be pulled into political narratives or cross-border disputes through misinformation campaigns, coordinated online harassment, or politicized media reporting. Managing communications, evidence, and legal positioning becomes a core responsibility.

For these reasons, geopolitical pressure is rapidly becoming a defining feature of corporate risk management in the Indo-Pacific. The challenges extend well beyond traditional legal counsel; they require integrated coordination between legal, cybersecurity, strategy, government-affairs, and executive teams. The GCs who succeed in this environment are those who anticipate geopolitical shifts, incorporate them into corporate governance and incident-response planning, and maintain proactive relationships with government agencies, regulators, and trusted security partners.

5. Board-level understanding and accountability.
Regulators in Japan and elsewhere may be increasingly expecting boards to articulate their organization's cyber posture and AI governance approach. GCs may be required to serve as the bridge between technical teams, senior management, and non-technical directors, ensuring alignment and informed decision-making.

Where do you see the strongest collaboration opportunities between Japanese companies and their U.S./European counterparts in areas like defense tech, cloud, fintech, or manufacturing?

There is a great deal of low-hanging fruit in collaboration between Japanese companies and their U.S./European counterparts. A few areas where I see the most traction:

1. Defense tech.
- Defense capabilities and ISR, autonomous systems, space-based sensing, and multi-domain ISR are all areas where the U.S./European technology can combine with Japanese industrial capability and Indo-Pacific geography. Japan's security reforms and alliance posture make it a natural partner in this space.

2. Active cyber defense and threat intelligence.
With the Active Cyber Defense Law and economic-security regime as a backdrop, there is room for joint development of:

- threat-intel platforms tailored to Japanese critical infrastructure,
- co-managed SOC services, and
- red-team/blue-team exercises that blend Western methodologies with Japanese regulatory requirements.

3. Cloud, data and AI.
- Japan has strong cloud adoption in regulated industries, but there is still a need for:
- sovereign-friendly architectures,
- AI security and governance solutions aligned to Japanese guidelines, and
- multilingual, Japan-specific models and analytics for cyber, fraud and compliance.

4. **Fintech and RegTech.**
   As Japanese financial institutions internationalize and face more complex cyber, AML, and sanctions-related obligations, Western Fintech/RegTech providers can partner with Japanese banks and insurers on:

   - secure digital onboarding,
   - transaction-monitoring enhanced by AI,
   - and integrated cyber-risk scoring for counterparties.

5. **Manufacturing, OT and supply-chain security.**
   - Japanese manufacturers bring world-class OT environments and a strong safety culture; Western partners bring advanced OT monitoring, vulnerability management, and attack-surface management tools. The CPSF-based guidelines effectively provide a shared "language" for these collaborations.

In all of these areas, the key is co-design: solutions that respect Japanese legal, cultural and operational realities, rather than simply "importing" a U.S. or European model. When you get that right, Japan is not just another market, it becomes a partner and a testbed for the broader Indo-Pacific.

News in Brief

Japan's New Prime Minister Signals Policy Shift

Sanae Takaichi elected PM as Japan pivots toward assertive economic and security agenda.

Japan appointed Sanae Takaichi as Prime Minister on 21 October 2025, following her victory in the Liberal Democratic Party leadership race and confirmation by the Diet. She becomes Japan's first female prime minister at a time of heightened regional and economic pressure. Takaichi moved quickly to form a cabinet combining fiscal conservatives with national-security hawks, signaling continuity on economic reform alongside a firmer stance on defense and foreign policy.

Markets initially reacted cautiously, with government officials stressing stability and disciplined fiscal management to avoid disruption. The appointment marks a leadership reset in Tokyo as Japan grapples with slowing growth, geopolitical tensions, and growing alignment with U.S. and allied security priorities.

Read more in Reuters.

Japan Accelerates Defense Spending to Meet NATO Benchmark

Tokyo targets 2% of GDP defense spending ahead of schedule under new government.

Japan's new government confirmed on 24 October 2025 that it will accelerate defense spending to reach 2% of GDP, moving the target forward from its original 2027 timeline. The increase supports missile defense, cyber capabilities, joint operations with U.S. forces, and enhanced maritime security amid rising regional tensions. Officials framed the move as essential to deterrence and alliance credibility rather than militarization, though it represents one of the most significant shifts in Japan's post-war security posture.

The spending push builds on Japan's multi-year defense build-up and reinforces its position as a key security partner in the Indo-Pacific.

Read more in Reuters.

U.S.–Japan Tariff Deal Weighs on Japan's Growth

Reduced auto tariffs fail to prevent first economic contraction in over a year.

Japan's economy contracted 1.8% year on year in the July–September 2025 quarter, marking its first contraction in more than a year, as U.S. tariffs continued to weigh on exports despite a recently concluded bilateral trade deal. Exports fell 1.2%, led by a sharp slowdown in automobile and auto-parts shipments.

The contraction follows the July 2025 U.S.–Japan trade agreement, under which Washington agreed to apply a 15% blanket tariff on Japanese exports, down from previously threatened levels of up to 27.5%, while retaining 50% duties on steel and aluminum. In return, Japan committed to approximately USD 550 billion in U.S. investments and agreed to increase purchases of American agricultural products, including rice.

Economists note that while the deal eased worst-case trade fears, the remaining tariff burden continues to damage Japan's most important export sector. Earlier strength in exports was driven by front-loading ahead of tariff hikes, a temporary cushion that has now faded. Automakers have moved into cost-cutting mode, raising concerns over slower investment, weaker wage growth, and subdued hiring.

With private consumption effectively flat amid persistently high food and energy prices, the government is preparing a supplementary budget focused on household support and strategic investment in areas such as AI, semiconductors, and shipbuilding. The fragile outlook is also expected to constrain the Bank of Japan's ability to raise interest rates above its current 0.5% level.

Read more in The New York Times.

Japan M&A Market Hits Record – Surges to USD232 billion in H1 2025

Japan's M&A Market Booms in 2025 — Deal-making surged to a record US$232 billion in the first half of 2025, making Japan a major driver of Asia's rebound in merger & acquisition activity.

This surge was fueled by a wave of large-scale take-private deals, outbound acquisitions, and a rise in private-equity–backed transactions - underpinned by historically low interest rates, corporate-governance reforms aimed at tackling undervaluation, and growing investor appetite for Japanese assets.
Bankers and dealmakers cited continued momentum into the second half of 2025, pointing to a strong pipeline of deals - from carve-outs and privatizations to cross-border transactions - keeping Japan firmly in the spotlight for global M&A.

Read more in Reuters.

Japan plans stricter terms for visas to foreign entrepreneurs

Japan's real estate sector achieved a significant milestone in Japan plans to tighten the terms of its Business and Management visa for foreign entrepreneurs by October 2025, raising the minimum capital requirement six-fold from ¥5 million to ¥30 million (about USD 204,000) and obliging applicants to hire at

least one full-time employee, rather than allowing capital investment or staffing alone to qualify. The visa, which permits stays of up to five years and can lead to permanent residency, was designed to attract global talent and innovation but has grown sharply in use, with around 41,600 holders by the end of 2024—over half of them Chinese nationals.

The move follows political pressure after gains by an anti-immigration party in the recent upper house election, which saw the ruling coalition lose its majority. Public feedback on the proposed changes is open until September 24, underscoring the government's balancing act between fostering entrepreneurship and tightening immigration rules.

Read more in Reuters.

Tokyo Launches Global MedTech Bridge

TOKYO SUTEAM selects international consortium to connect Japanese medtech startups with Silicon Valley.

A consortium comprising Investable Solutions, Nozomi MedAlliance K.K., and Theranova, LLC has been selected as an official partner of TOKYO SUTEAM, the Tokyo Metropolitan Government's flagship startup support initiative, announced in 2025 as part of a globally competitive cohort of 50 partners. Through the Tokyo–Silicon Valley MedTech Launchpad, the program focuses on sourcing and supporting high-potential Japanese medtech and medical device startups with serious global ambitions, particularly in the United States.

The initiative provides hands-on access to overseas regulatory pathways, including FDA strategy and pre-submissions, validation of technology and intellectual property, and direct collaboration with Silicon Valley investors, hospitals, and innovation ecosystems. Designed for startups based in Tokyo or considering relocation, the launchpad aims to deliver tangible outcomes such as patent filings, regulatory progress, and strategic business alliances.

The program positions itself as a proven bridge between Japan's advanced medical technologies and global markets, supporting founders with world-class IP who are actively pursuing international expansion.

Read more and apply:
www.tokyomedtech.com

One of the largest Japan-UK medtech deals

In August 2025, Japan's Terumo Corporation signed a definitive agreement to acquire Oxford University spin-out OrganOx Ltd. for around USD 1.5 billion, marking one of the largest UK medtech exits to date and the biggest sale of an Oxford spin-out.

The deal, still pending U.S. regulatory approvals before completion, represents Terumo's first entry into the organ transplantation sector, expanding its established global portfolio in cardiac, vascular, and hospital devices.

OrganOx's flagship metra® normothermic perfusion device, already used in over 6,000 liver transplants worldwide and approved across the U.S., EU, UK, Canada, and Australia, enables extended preservation and real-time viability assessment of donor organs. For investors, notably BGF, the exit delivered a 10x return and a ~69% IRR, underlining its scale compared to prior medtech deals in Europe.

This transaction positions Terumo alongside other global medtech leaders pursuing high-growth transplantation innovations, cementing OrganOx's role as a transformative player in the field.

Japan Bets Big on India: ¥10 Trillion Target Set

Japan is preparing to double down on its economic partnership with India, setting a bold new target of ¥10 trillion (USD 68 billion) in private-sector investment over the next decade. The move, which significantly raises the bar from the ¥5 trillion goal announced in 2022, comes just ahead of Prime Minister Narendra Modi's visit to Japan, where he will meet his counterpart, Prime Minister Shigeru Ishiba, from August 29 to 30, 2025.

The summit agenda highlights the strategic weight of the relationship, with joint appearances and a site visit in Miyagi Prefecture showcasing Shinkansen test-vehicles and semiconductor equipment. Alongside the headline pledge, Tokyo and New Delhi are introducing two new frameworks: an Economic Security Initiative to bolster supply chain resilience across semiconductors, rare earths, communications, clean energy, AI, and pharmaceuticals; and an AI Cooperation Initiative to strengthen collaboration in artificial intelligence, including startup development and emerging technologies. These measures underscore how both nations aim to reinforce their partnership at the intersection of technology, security, and economic growth, positioning themselves as pivotal players in regional and global supply chains.

Read more in Japan Forward.

QIA and KKR Back Japanese Relisting

Qatar Investment Authority and KKR invest as SBI Shinsei Bank prepares for Tokyo Stock Exchange return.

SBI Shinsei Bank is set to return to the Tokyo Stock Exchange in December 2025, with Qatar's sovereign wealth fund, the Qatar Investment Authority (QIA), and U.S. private-equity firm KKR taking stakes ahead of the relisting. The investment strengthens the lender's capital base and brings in two major global institutional backers as the bank re-enters public

markets after its earlier delisting under SBI Holdings.

The relisting follows a multi-year restructuring process and is expected to be one of Japan's largest IPO-type transactions of the year. Reuters reported on 13 June 2025 that SBI Shinsei planned to file for relisting by year end as part of its turnaround strategy, and on 8 December 2025 that the bank priced its offering at the top of the indicated range, raising approximately JPY 370 billion, with trading due to begin on 17 December 2025. The participation of QIA and KKR underscores continued foreign investor confidence in Japan's financial sector and highlights the growing role of private capital in supporting bank recapitalizations and market re-entries.

Japanese Offshore Wind Setback

Mitsubishi-led consortium exits offshore wind projects in Japan.

A Mitsubishi Corporation–led consortium has confirmed its decision to withdraw from three major offshore wind power projects in Japan, covering sites in Chiba and Akita prefectures with a combined capacity of approximately 1.76 GW and planned operations between 2028 and 2030. The projects were originally awarded in Japan's 2021 offshore wind auction and formed a core part of the country's push toward renewable energy deployment.

The exit reflects a sharp deterioration in project economics since the original bids, driven by surging construction and material costs, supply-chain disruptions, a weaker yen, and higher interest rates. Mitsubishi and its partners concluded that the original assumptions underpinning the bids were no longer viable. The withdrawal has also resulted in impairment charges for Mitsubishi, with consortium partner Chubu Electric Power flagging related losses.

The development represents a significant challenge for Japan's offshore wind ambitions, which target 10 GW by 2030 and 45 GW by 2040, and has prompted government discussions around auction reform and potential re-tendering of the affected sites under revised terms to restore investor confidence.

Read more in Reuters.

Nissan Restructures as Tariffs Bite

Japanese automakers diverge as U.S. trade deal helps peers but Nissan deepens turnaround.

Japan's auto sector has seen mixed fortunes in recent months. While major manufacturers such as Toyota and Honda received a boost after the U.S. and Japan agreed to reduce auto import tariffs, Nissan Motor Co. has come under sustained pressure, reporting significant losses and accelerating its restructuring programme. In July 2025,

Reuters reported that Nissan posted its first quarterly operating loss in more than four years, driven by U.S. tariffs, weaker demand, and rising costs, prompting the company to cut global production capacity and pursue aggressive cost-reduction measures.

Nissan has announced plans to shutter its Oppama plant by March 2028, shift production to Kyushu, and reduce its workforce significantly, as part of a broader effort to stabilize cash flow and refocus operations. Production disruptions linked to chip and battery shortages have also weighed on output, including scaled-back plans for the next iteration of the Leaf electric vehicle. At the same time, Nissan has sought longer-term efficiencies through technology, expanding joint AI initiatives aimed at shortening vehicle development cycles.

The contrast with peers underscores broader structural changes in Japan's auto industry: while tariff relief and stable demand have supported some manufacturers, others face sharper exposure to trade friction, supply-chain volatility, and the capital demands of the EV transition.

NÍSHLÍS

10 Years | GLOBAL LEGAL MARKETING

Nishlis is a leading global legal marketing company with headquarters in London and offices in Tokyo, Helsinki, Tel Aviv and Warsaw and an affiliate in New York City. Established in 2014, the company leverages its extensive experience within major global law firms and publishers to provide comprehensive marketing solutions to law firms.

As your trusted consultant, we draw on expertise accumulated at the largest law firms globally and the most prominent legal directories to provide you with insights to make that leap, compete effectively and be noticed by the very clients you are looking to win.

Global Reach

Key Services

- Marketing Strategy
- Submissions for Legal Directories
- International Business Development
- Strategic Communications
- Professional Development

What makes us stand out - Global, Strategic, Holistic

Contact Us

nishlis.com
idan@nishlis.com
+44 (0)7475532261
+44 (0)2038111415

Firm News
and Updates

Japan's Top Food & Beverage PE Deal of 2025

MoFo advises Affinity Equity Partners on landmark Japanese acquisition
Affinity Equity Partners has completed one of Japan's most significant private equity transactions of 2025 in the food and beverage sector, marking a standout deal in a highly competitive market. The transaction underscores continued investor appetite for high-quality consumer brands in Japan and reflects growing confidence in the sector's long-term growth prospects amid inflationary pressures and changing consumer demand.

Morrison Foerster advised Affinity Equity Partners on the deal, which was led by Gary Smith and Mitsutoshi Uchida, alongside colleagues from across the firm's Japan and global platform.

Japan's AMT and SMBC Group Launch Major Legal Tech Platform

A new legal-tech joint venture has been launched in Japan with the establishment of SMBC LegalX Co., Ltd., aimed at delivering end-to-end Contract Lifecycle Management (CLM) services through an AI-driven platform. The initiative brings together Anderson Mori & Tomotsune (AMT), SMBC Group, Volody Products Pvt Ltd and LexisNexis Japan, marking what the parties describe as the largest alliance to date in Japan's legal-tech sector.

The new "LegalXross" platform is designed to digitize the entire contract process, from creation to management and analysis, responding to rapid advances in AI and increasing demand for efficiency and scalability in legal operations. SMBC, AMT and Volody have also agreed to enter into a capital and business alliance, with plans to invest in SMBC LegalX by the end of 2025. This represents the first-ever capital and business alliance between a major Japanese bank and a leading domestic law firm.

The initiative reflects a broader shift within Japan's legal market towards technology-enabled service models and positions the venture with global ambitions in the CLM space. The announcement was supported by comments from Maki Kadonaga, Partner and Chief Knowledge Officer, and Wataru Shimizu, Partner at Anderson Mori & Tomotsune, highlighting the firm's strategy to combine deep legal capability with advanced technology to drive long-term transformation.

Japan's Mori Hamada & Matsumoto Expands into London Market

In September, the Japanese law firm announced its London plans as part of global strategy. AMT opened in London in 2023; Nishimura & Asahi opened in 2024.

Mori Hamada & Matsumoto has announced plans to open a London office in 2026, marking a significant step in the firm's continued international expansion and its push to deepen engagement with global clients. The move reflects growing demand for Japanese legal expertise in cross-border transactions involving Europe, Asia, and beyond, particularly across M&A, finance, disputes, and regulatory matters.

London was selected for its role as a leading global legal and I financial hub, offering proximity to international financial institutions, private equity sponsors, and multinational corporations. The new office is expected to strengthen the firm's ability to advise on complex international transactions and disputes, while acting as a bridge between Europe and Japan.
The expansion builds on Mori Hamada's existing overseas presence, including offices across Asia and in New York.

The announcement underscores a broader trend among leading Japanese law firms to internationalize their platforms and compete more directly with global firms on outbound Japanese work and inbound international mandates.

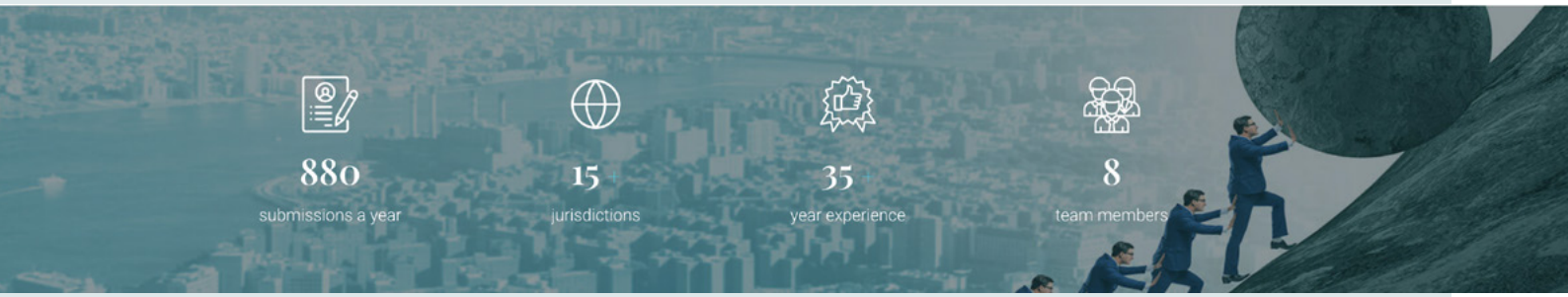
Tier One
RANKINGS by NÍSHLÍS | GLOBAL LEGAL MARKETING

Let us help improve the odds for your firm and your lawyers to earn the recognitions they deserve.

Tier One Rankings has only one focus: to help you succeed with your directories and awards submissions.

Services

- Submissions Outsourcing
- Submissions Editing
- Strategic Content Creation
- Workshops



Contact us

NISHLIS
10 Years | GLOBAL LEGAL MARKETING

WWW.NISHLIS.COM ⁄ NISHLIS@LEGALMARKETING.CO.IL
TEL. +81(0)80 5688 5029 ⁄ FOLLOW US:

Designed by ELEMENT