YAVA MONTHLY REPORT

DATE: 30.04.2026

ISSUE NO. 18



# INSIDE THIS ISSUE


PG. 2-3
Why real-world risk visibility is becoming essential

PG. 4
Infrastructure security trends and AI & risk intelligence

PG. 5
Aviation and airport resilience

PG. 6
Global deployment in action: AI infrastructure

PG. 7
Partnerships, resilience, and market outlook


## YAVA Monthly Report

Welcome to YAVA's Monthly Report, offering a clear snapshot of our latest projects, regional developments, and sector movements. Each edition includes YAVA project updates, market analysis, and key news from Africa, the Middle East, India, and Europe — delivering practical insight across our operating landscape.

Visit www.yava.com for more.
Or follow us on LinkedIn (@YAVA_COM)



Markets, industries, and organisations increasingly require real-world visibility into how assets function, not simply how they are described on paper, as operational exposure becomes harder to assess through declared data alone.

## War and Geopolitical Developments

- **Red Sea disruption continues to pressure trade routes:** Renewed attacks on commercial shipping and maritime security operations have sustained pressure on one of the world's most important trade corridors, increasing insurance and logistics costs.
- **Ukraine strikes keep energy infrastructure in focus:** Continued attacks on refining, storage, and power assets have reinforced how energy systems remain central targets in modern conflict.
- **South China Sea tensions raise infrastructure exposure:** Increased naval activity and diplomatic friction have renewed focus on shipping lanes, subsea cables, and strategic industrial supply routes across Asia.

## BEYOND INSURANCE

**From reported risk to real-world understanding**

Across infrastructure, energy, logistics, hospitality, and complex asset markets, a growing gap is emerging between reported risk and real-world exposure. Traditional underwriting and investment assessments still rely heavily on declared data, desktop modelling, historical assumptions, and standardised questionnaires. Yet in high-growth and high-risk environments, those inputs often fail to capture the true condition of assets on the ground.

This matters because infrastructure risk is increasingly operational. Cyber vulnerabilities, weak access control, fragile utilities, poor redundancy, and limited technical oversight may not be visible at placement stage, but they can determine whether an asset remains functional during disruption.

According to the Allianz Risk Barometer 2026, cyber incidents remain the top global business risk, while business interruption and natural catastrophe continue to rank among the most material threats to enterprise performance. This reflects a wider shift: risks once treated separately are now converging.

YAVA's developing risk intelligence model reflects this change. The aim is to move from declared risk to observed, verified risk by embedding technical assessment, on-site visibility, and remediation capability into the risk evaluation process.

Three structural dynamics are becoming increasingly visible:

- **Declared data is no longer enough:** Asset owners, insurers, and investors increasingly require verified insight into the real condition of cyber, physical, and infrastructure systems before risk can be accurately priced or managed

- **Risk engineering is moving closer to commercial decisions:** Marsh notes growing demand for stronger resilience frameworks and operational visibility as organisations reassess how risk is transferred and mitigated

- **Resilience must be measured operationally:** The key question is no longer whether controls exist, but whether systems can continue functioning under stress

This convergence of insurance, engineering, and infrastructure resilience is reshaping how risk is understood in practice. Risk intelligence is no longer simply about identifying exposure after the fact. It is becoming a tool for improving insurability, strengthening asset performance, and reducing loss before disruption occurs.


Copyright © 2026

## Related Topics

- Allianz says cyber incidents remain the top global business risk, ahead of business interruption and natural catastrophe (Allianz Risk Barometer 2026)
- Meta's new Tulsa data centre includes $25 million of local roads and water upgrades, highlighting how infrastructure delivery now extends beyond the asset itself (Reuters)
- UK 'powered land' rush accelerates as dormant industrial sites are repurposed for AI data centres, reflecting how real-world asset readiness is driving value (Reuters)
- European industrial and electrical stocks rally on AI-linked demand for grid equipment and data-centre infrastructure (Reuters)



Operational resilience depends on visibility, coordination, and systems that function together under pressure.

# FROM INSIGHT TO EXECUTION

**YAVA and Compass Point's strategic partnership is turning insight into delivery**

Across insurers, operators, investors, and infrastructure stakeholders, one message is becoming increasingly clear: resilience is rarely delivered by one organisation alone. As risk environments become more complex, the ability to combine specialist capability through trusted partnerships is becoming a competitive advantage.

This is where YAVA's strategic partnership with Compass Point is particularly important.

Compass Point brings established expertise in insurance advisory, risk placement, market access, and strategic relationships across sectors where resilience, underwriting confidence, and operational visibility are increasingly connected. Combined with YAVA's engineering, deployment, and infrastructure execution capability, the partnership creates a stronger bridge between risk insight and real-world delivery.

Together, the partnership is designed to support organisations seeking stronger outcomes across:

- Risk visibility and operational due diligence
- Insurance readiness and improved insurability
- Infrastructure resilience planning
- Technical remediation and systems upgrades
- Market access through trusted advisory networks
- Multi-region execution in complex environments

A second pillar of the relationship is the development of a joint affiliate partnership programme. This model is intended to create a broader ecosystem of advisers, brokers, technical specialists, introducers, and regional partners who can identify client needs early and connect them to delivery capability quickly.

As infrastructure risk becomes more interconnected, clients increasingly need coordinated solutions rather than isolated services. The affiliate programme is designed to meet that demand by expanding trusted routes to market while maintaining quality of execution.

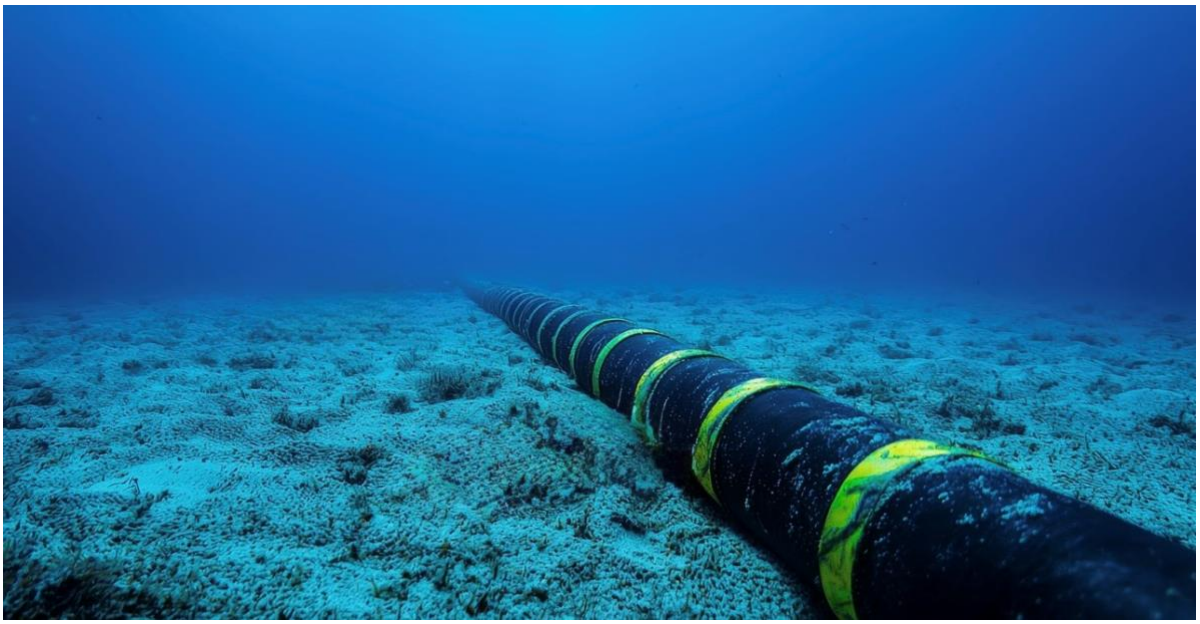
Three structural advantages are emerging:

- **Broader market reach:** Stronger access to clients and sectors where resilience demand is rising rapidly
- **Faster conversion from insight to action:** Risk issues identified earlier can move faster into funded remediation and implementation
- **Integrated client outcomes:** Advisory, insurance, and engineering capabilities can be aligned around one operating objective

For YAVA, this reflects a wider principle: strategic partnerships matter most when they translate capability into results.

COMPASS POINT
ASSIST


Copyright © 2026



Subsea cable resilience is rising up the security agenda, as governments respond to growing concern over sabotage, surveillance, and disruption to critical digital infrastructure.

## INFRASTRUCTURE SECURITY TRENDS TO WATCH

**Hybrid threats continue to reshape exposure**

- **AI-assisted cyberattacks are accelerating:** Automated phishing, malware generation, and reconnaissance tools continue lowering the cost and speed of attacks across infrastructure operators (World Economic Forum)

- **Subsea cable resilience moves higher:** Governments and telecom operators continue expanding contingency planning around cable disruption and maritime sabotage risk (Reuters)

- **Energy systems remain strategic targets:** Reuters reported that Russia was forced to cut oil output in April following Ukrainian drone attacks on ports and refineries, alongside disruption to crude supplies through its remaining pipeline route to Europe (Reuters)

- **Insurance scrutiny is increasing:** Underwriters are requesting stronger evidence of continuity planning, cyber hygiene, and operational controls before binding cover (Marsh)

- **Supply chain disruption remains persistent:** Weather shocks, trade friction, and route concentration continue to affect industrial delivery timelines (World Economic Forum)

- **Critical communications networks face rising pressure:** Internet outages in Russian cities disrupted banking, transport and everyday services in April, highlighting how communications networks are becoming operationally critical during security crises (Reuters)

## TECHNOLOGY HIGHLIGHT: AI and RISK INTELLIGENCE

**Smarter systems moving from efficiency to resilience**

AI is accelerating the shift from reactive risk management toward predictive resilience.

Across infrastructure, insurance, logistics, and asset-heavy sectors, AI tools are improving the ability to detect anomalies, assess vulnerabilities, and model disruption before losses occur. What began as an efficiency tool is increasingly becoming an operational resilience layer.

Key growth areas include:

- Predictive maintenance for critical assets
- Threat detection across cyber and physical systems
- Route disruption modelling
- Automated compliance monitoring
- Real-time incident decision support

According to McKinsey, AI has the potential to make maintenance operations more reliable, efficient and cost-effective by improving operator support, preventive strategies and troubleshooting.

The value increasingly lies in integration. AI systems connected to real operational workflows can strengthen continuity and improve decision-making under pressure.

Used effectively, AI supports resilience. Used poorly, it can increase dependency on weak systems and poor data.


Copyright © 2026



Airports are increasingly judged not only by capacity, but by their ability to maintain continuity during disruption, security incidents, system failure, and rising pressure on critical infrastructure networks.

# SPOTLIGHT: AVIATION AND AIRPORT RESILIENCE

**Continuity in high-pressure operating environments**

Airports and aviation systems are increasingly positioned at the centre of economic continuity, sovereign reputation, and operational risk. They are no longer simply transport assets; they are interconnected infrastructure environments where security, logistics, technology, and public confidence converge.

Modern airports rely on tightly integrated systems: passenger flows, baggage handling, fuel supply, access control, air traffic coordination, digital networks, and real-time communications. Disruption in one layer can rapidly affect the whole operating environment.

This creates growing pressure across four areas:

- **Operational continuity:** Airports must maintain throughput despite security alerts, weather shocks, technical failures, labour disruption, or geopolitical volatility.

- **Cyber-physical convergence:** Increasing digitisation improves efficiency, but expands attack surfaces across connected operational technology and enterprise systems.

- **Passenger growth vs capacity pressure:** ACI World forecasts global passenger traffic to reach 10.2 billion in 2026, with long-term demand projected to rise to 18.8 billion by 2045, increasing pressure on infrastructure capacity and resilience planning.

- **Passenger confidence and reputation:** Delays, outages, or visible failures can have immediate commercial and political consequences.

Recent industry commentary also highlights the cost of disruption. According to Eurocontrol and ACI Europe reporting, delays linked to airspace congestion, staffing constraints, and operational bottlenecks continue to weigh on airport performance across key markets.

Three structural realities are becoming clear:

- Airports are critical national infrastructure, not just transport hubs
- Digital systems and physical operations can no longer be managed separately
- Resilience investment increasingly protects revenue as much as security

For operators, the focus is shifting from expansion alone to resilience by design.

That means integrating secure communications, redundancy across critical systems, real-time visibility, and coordinated incident response into daily operations rather than treating resilience as a contingency layer.

Airports must not only move passengers efficiently. They must remain functional under pressure.



Modern aviation depends on tightly integrated physical and digital systems, where disruption in one layer can rapidly affect the wider operating environment.


Copyright © 2026

## Related Topics

- Microsoft deepens commitment to Australia with A$25 billion investment in AI infrastructure, security, and skills (Microsoft)
- Microsoft and OpenAI Restructure Partnership to Accelerate Global AI Infrastructure and Multi-Cloud Expansion (TechAfrica News)
- Green AI infrastructure market to hit $61 billion by 2035 (Precedence Research)
- Meta partners with space startup Overview Energy to secure solar power for data centers (Reuters)
- Oracle data center $16 billion financing gets over the line (Bloomberg)
- China's data center capacity set to top 60 GW by 2030, driving a doubling of power demand (RystadEnergy)
- Strategic framework proposed for data center applications in the state of Lower Austria (Data Center Dynamics)

**Strategic partnership expands security and operational capability**

As infrastructure risk becomes more physical, fragmented, and geopolitically exposed, technical resilience alone is no longer enough. Clients increasingly require integrated delivery models that combine cyber capability, engineering systems, operational security, logistics support, and on-the-ground execution.

This is the strategic context behind YAVA's partnership with Salama Fikira Group.

The partnership creates a two-way commercial model designed to combine complementary strengths. Salama Fikira introduces YAVA into client environments requiring technology, cyber, systems audits, and operational intelligence capability. In parallel, YAVA introduces Salama Fikira into its own client relationships where physical security, transport, protection, and field operations capability are required.

This creates a stronger client proposition across complex markets where resilience depends on both digital and physical layers operating together.

This is especially relevant in regions where clients face overlapping exposure across security, infrastructure, supply chain, and technology environments. In these settings, resilience is not delivered through isolated advisory work, but through trusted partners who can assess risk, mobilise capability, and support implementation on the ground.

Together, the partnership supports delivery across:

- Operational security and protective services
- Cyber and systems audits
- Infrastructure assessments
- Logistics and transport support
- Technical deployments in higher-risk markets
- Ongoing support across shared client environments

A key advantage is commercial alignment. Both firms participate in long-term value of introduced client

# GLOBAL DEPLOYMENT IN ACTION

relationships, creating incentives around performance, trust, and continuity rather than one-off transactions.

Three structural advantages are clear:

- **Integrated delivery:** Clients can access technical and operational capability through one trusted route.
- **Stronger market access:** Each firm expands into new sectors and client networks through partnership.
- **Better resilience outcomes:** Cyber, physical security, and operational systems can be delivered together rather than separately.

As infrastructure risk becomes more interconnected, partnerships that combine specialist capabilities are likely to outperform siloed service models.

For YAVA, the Salama Fikira partnership reflects a wider strategy: building ecosystems that translate capability into scalable delivery.





Copyright © 2026



# LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

### Resilience becomes a commercial advantage

April developments reinforce a wider market reality: resilience is increasingly commercial.

Infrastructure owners want continuity. Insurers want visibility. Investors want certainty. Governments want stability.

No single organisation controls the full resilience stack required to deliver these outcomes.

Energy systems depend on communications networks. Airports rely on cyber controls and logistics continuity. Commercial assets require utilities resilience, insurance capacity, and operational governance.

The next phase of growth will belong to organisations able to coordinate trusted systems across increasingly fragmented and interdependent markets.

This is creating demand for collaboration between:

- Operators and engineering firms
- Insurers and technical risk specialists
- Governments and private delivery partners
- Asset owners and multi-region implementation teams
- Technology providers and infrastructure operators

Organisations that adapt early to converging risk environments will outperform peers operationally and financially.

YAVA's focus remains clear: connecting engineering capability, operational intelligence, and deployment execution into systems designed to perform under pressure.

As uncertainty rises, resilience becomes more than protection.

It becomes a source of competitive and commercial advantage.

# YAVA's Event Calender

- **Data Centre and Cloud Infrastructure Expo**
  Kuala Lumpur, Malaysia | 12-13 May | Link
- **Smart Cities World Summit**
  London, UK | 24-25 Jun | Link
- **Gartner IT Infrastructure, Operations & Cloud Strategies Conference**
  London, UK | 16–17 Nov| Link

For enquiries relating to the topics, commentary, or content in this report, please contact our media team at media@yava.com

When emailing the media team, please use the subject line **"Media Team – Issue (Report Number)"** to help us respond efficiently.


Copyright © 2026

# Disclaimer and Confidentiality Notice

This monthly report (the "Report") is issued by YAVA London Ltd ("YAVA") on a confidential basis and is provided solely for informational and discussion purposes. It is intended exclusively for the designated recipient(s) and may not be copied, reproduced, redistributed, forwarded, quoted, or otherwise disclosed, in whole or in part, to any third party without YAVA's prior written consent.

The Report contains a curated summary of YAVA's activities, observations, and perspectives, including but not limited to: operational updates, regional and sector commentary, infrastructure and security themes, geopolitical context, execution insights, and internally derived assessments. Certain references may relate to governments, public authorities, private organisations, supranational bodies, or security-sensitive environments. Portions of the content may therefore be commercially sensitive, politically sensitive, operationally sensitive, or subject to confidentiality obligations.

By accessing, receiving, or reviewing this Report, the recipient acknowledges and agrees to the following conditions:

### Confidentiality and Restricted Use

All information contained herein is confidential and proprietary to YAVA. The Report is provided for the recipient's internal use only and must not be used for external briefing, publication, marketing, solicitation, or secondary analysis without YAVA's express written approval.

### Non-Circumvention and Relationship Protection

Recipients agree not to directly or indirectly contact, solicit, engage, or seek to establish independent relationships with any clients, counterparties, partners, stakeholders, or entities referenced in the Report. Any attempt to circumvent YAVA's role in current or prospective engagements may constitute a material breach and may give rise to legal or equitable remedies.

### No Offer, No Advice, No Reliance

This Report does not constitute, and should not be construed as, an offer, solicitation, recommendation, or endorsement of any service, engagement, transaction, or course of action. It does not provide legal, regulatory, operational, or professional advice. Nothing in this Report creates or implies any advisory, fiduciary, contractual, or agency relationship between YAVA and the recipient.

### Observational Commentary and Forward-Looking Content

The views, commentary, and thematic analysis expressed reflect YAVA's observations and internal perspectives as of the date of publication. Certain statements may be forward-looking or indicative in nature and are inherently subject to uncertainty, evolving conditions, and factors outside YAVA's control. Actual outcomes may differ materially from any expressed or implied views.

### Sources and Accuracy

Information contained in this Report may be derived from a combination of publicly available sources, partner discussions, governmental communications, industry dialogue, and YAVA's internal activities. While such sources are believed to be reliable, YAVA does not represent or warrant the accuracy, completeness, or continued relevance of the information, and undertakes no obligation to update or revise the content.

### Limitation of Liability

To the fullest extent permitted by law, YAVA, its directors, officers, employees, consultants, and affiliates shall not be liable for any loss, damage, cost, or expense, whether direct, indirect, incidental, or consequential, arising from the use of, reliance upon, or interpretation of this Report or its contents.

### Governing Law and Jurisdiction

This Report and any matters arising from or relating to its use shall be governed by the laws of England and Wales. The courts of London, United Kingdom, shall have exclusive jurisdiction.


Copyright © 2026