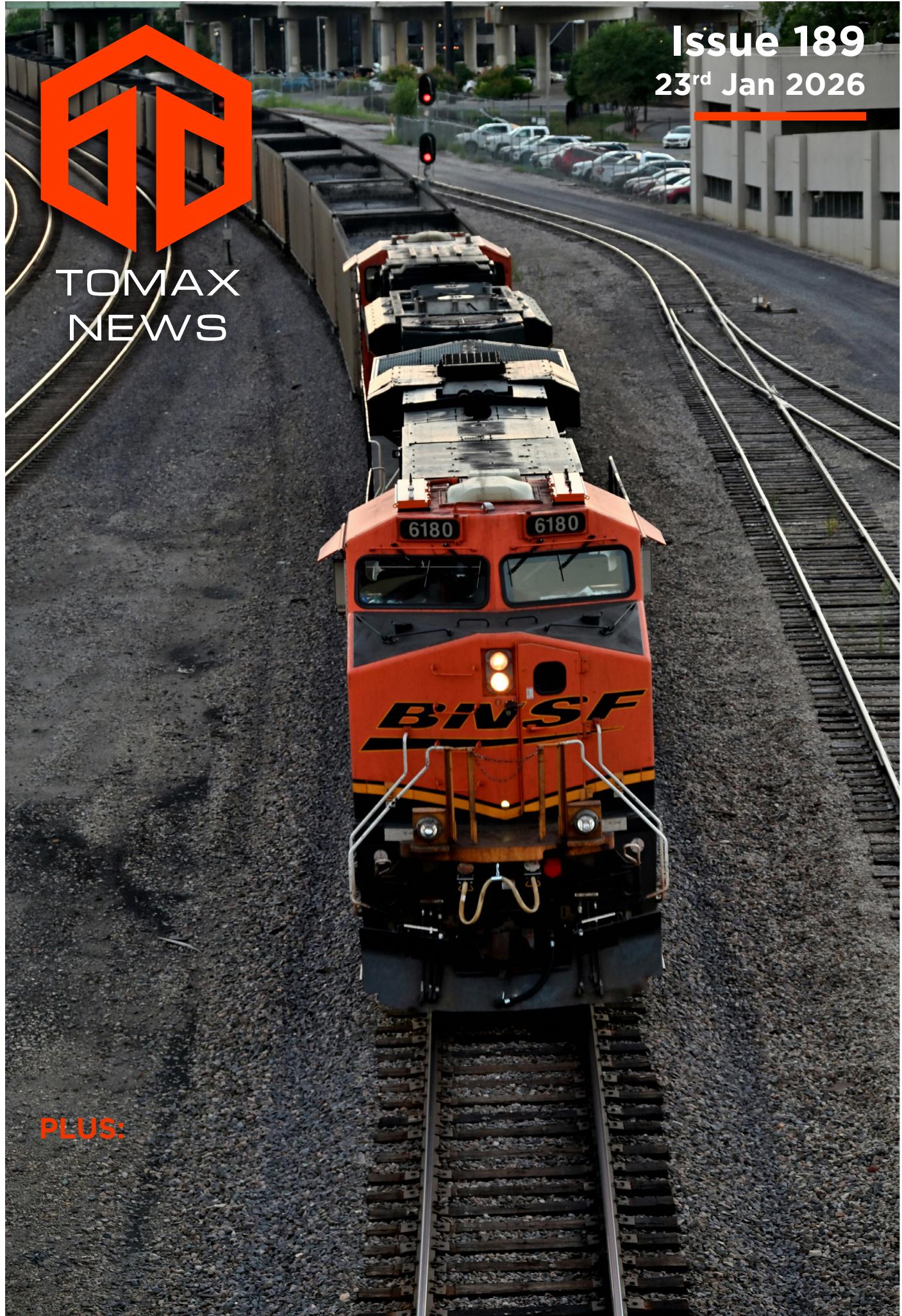




TOMAX  
NEWS

Issue 189  
23<sup>rd</sup> Jan 2026



**PLUS:**

# MARKET SUMMARY

- Welcome to 2026!! The entire Tomax team hopes you had a nice Christmas and New Years break, and are feeling refreshed and ready for a big year in 2026! We're excited to be here working alongside you once again. Thank you for the continuing support which we appreciate greatly! Stay tuned for more improvements to the Tomax Live system this year as we make it more and more powerful.
- Shipping lines have begun using the Suez Canal more and more as tensions begin to ease. Not all lines have returned to the shorter transit lane and some are

continuing to use alternate routes. Your Key Account Manager will be in touch with you regarding the changes to the European shipping options.

- Freight rates from China to Australia are dropping as cargo volumes are weak in the lead up to the late February Chinese New Year period this year. There will no doubt be a strong surge of bookings as we head into mid-February so please work with your suppliers to have orders ready as early as possible if you are seeking to ship prior to the CNY period.

## TARIFF CONCESSIONS GAZETTE (TC)

Tariff Concession Orders (TCOs) are an Australian Government revenue concession that exists where there are no known Australian manufacturers of goods that are substitutable for imported goods.

[CLICK TO VIEW LATEST GAZETTE](#)





# RISING CYBER RISKS IN SUPPLY CHAINS

**S**upply chain leaders are grappling with an increasingly complex and near-impossible task: strengthening cyber security defences while simultaneously pushing for greater visibility and integration across their networks. While digital integration brings efficiency gains, it also creates a wider attack surface, opening up more entry points that are difficult to secure with traditional safeguards alone.

The threat landscape is escalating rapidly. According to Everstream Analytics' 2026 Annual Supply Chain Risk Report, cyber attacks targeting logistics are expected to double this year. The report found that incidents affecting carriers, ports and logistics providers have surged by nearly 1,000% since 2021. In 2025 alone, Everstream recorded 213 such incidents, representing a 61% increase from the 132 reported in 2024.

Supply chains are particularly attractive targets for cyber criminals due to their growing number of interconnected systems, which offer multiple points of vulnerability to exploit. Logistics networks are also viewed as a gateway into the core operations of cargo owners, amplifying their appeal to attackers. The inherent complexity of supply chains, combined with the sheer number of participants involved, makes them especially difficult to protect. SecurityScorecard's 2025 Supply Chain Cybersecurity Trends report highlights this challenge, noting that 79% of

organisations said fewer than half of their external vendors were covered by formal cyber security programmes. Furthermore, 28% of surveyed organisations experienced cyber incidents over the past two years that originated from vulnerabilities in third-party vendors.

Additional risks stem from the increasing use of IoT and automation devices, which often rely on software that is infrequently updated or protected by weak authentication measures. These devices present further access points for cyber criminals.

One cyber security expert noted that regulatory compliance and standard endpoint security controls are no longer sufficient to provide adequate protection. At the same time, threat actors are becoming more advanced, in some cases benefiting from state-level backing. The Everstream report observed that last year, "a growing number of incidents were linked to state-sponsored groups, with activity tied to Russia, China and Iran".

The authors also pointed to coordinated campaigns targeting maritime infrastructure, airport systems and transport networks across multiple countries. These attacks, they concluded, are "becoming more co-ordinated and harder to contain".

The scale and coordination of such incidents underscore another worrying trend: a shift

away from attacks on individual companies towards targeting entire networks. As digital connectivity to transport hubs and logistics nodes continues to grow, cargo owners and service providers face heightened exposure to attacks originating through these shared systems.

This evolving threat environment highlights the need for cyber security strategies that extend beyond isolated measures such as continuous supplier monitoring. While cyber supply chain risk management remains essential, a broader and more coordinated response is increasingly necessary, particularly in the face of state-sponsored activity. In the US, the Airforwarders Association has called on the Department of Transportation to establish a federal cargo theft and fraud task force led by the department and the Federal Motor Carrier Safety Administration, working in collaboration with the FBI and the Department of Justice. The association has also advocated for a national cargo theft database powered by AI, along with stricter carrier verification requirements.. However, the rapid adoption of AI is also introducing new risks. "As well as bringing

huge opportunities, AI's transformative potential and rapid evolution and adoption are also reshaping the risk landscape, making it a standout concern for firms of all sizes worldwide, alongside other more established threats," warned Allianz Commercial CEO Thomas Lillelund.

Allianz's latest Risk Barometer identifies the accelerated uptake of AI as one of the key drivers of increased risk exposure for businesses. "AI is supercharging threats, increasing the attack surface and adding to existing vulnerabilities," said Michael Bruch, the company's global head of risk consulting advisory services.

Putzger, I (2026). Traditional defences not enough as AI adds to cyber-attack risk. Retrieved from <https://theloadstar.com/traditional-defences-not-enough-as-ai-adds-to-cyber-attack-risk/> on 22nd January 2026.





# LUNAR NEW YEAR RESHAPES CHINA-AUSTRALIA SHIPPING

**T**he shape of container shipping's Lunar New Year response is shifting, with carriers abandoning a peak season surcharge while adding further voyage blankings on the China-Australia trade.

The A3 consortium—ANL, COSCO SL and OOCL—has confirmed that its A3C and A3S services, serving central and southern China respectively, will double the number of previously announced voyage cancellations. “Further to our advisory dated 14 January, please note A3C and A3S loops will have two-week slides as we anticipate a slowdown in southbound demand during Chinese New Year,” ANL said.

On the A3C service, sailings from OOCL Brazil 054S/N will be slid by two weeks, resulting in blank sailings in Shanghai on 19 and 26 February.

Meanwhile, the A3S service will see sailings from COSCO Hong Kong 204S/N also pushed back by two weeks, creating blank positions in Xiamen on 20 and 27 February.

ANL has also confirmed that its peak season surcharge (PSS) on shipments from North-

East Asia to Australia will be withdrawn effective 1 February.

Separately, adverse weather and port congestion on both sides of the Tasman have forced ANL to slide its four-vessel TranzTas service by one week, in a bid to restore schedule integrity. The adjustment will take effect from ANL Rotorua V2601/2602.

New Zealand schedules have remained disrupted for several weeks, with a steady stream of port omissions and rotation changes, primarily impacting Asian services.

Crisp, D. (2026). More CNY adjustments announced. Retrieved from <https://www.thedcn.com.au/news/more-cny-adjustments-announced> on 23rd January, 2026.



# CARGO DRUG CONCEALMENT EXPOSED

**M**osaic tiles, crane components, buses, high-value fabric and even consignments labelled as “vegetable spring rolls” are among the increasingly creative concealment methods used by criminal syndicates attempting to smuggle illicit drugs into Australia.

Throughout 2025, Australian Border Force (ABF) intercepted a wide range of illicit substances and precursors across air, mail and sea cargo streams destined for Australia. These seizures, carried out in conjunction with the Australian Federal Police (AFP), included:

- 9.2 tonnes of methamphetamine, with an estimated street value of \$5.5 billion
- 7.8 tonnes of cocaine, valued at approximately \$2.5 billion
- 6.3 tonnes of 1,4-butanediol, with an estimated street value of \$18.9 million
- 1.3 tonnes of ketamine, valued at around \$273 million
- 260 kilograms of MDMA, with an estimated street value of \$42.6 million
- 220 kilograms of heroin, valued at approximately \$110 million

Through ongoing collaboration, intelligence gathering and information sharing, Australian authorities continue to uncover the sophisticated concealment techniques employed by organised crime groups seeking to flood the Australian community with illicit drugs and cause widespread harm.

One of the most recent interceptions occurred at Port Botany in December 2025, when

ABF officers uncovered 22 plastic blocks containing a total of 27 kilograms of cocaine.

This followed an earlier seizure in October 2025, when approximately 145 kilograms of cocaine was discovered by ABF officers inside shipping containers in New South Wales.

AFP Commander Adam Rice said the AFP remained committed to working closely with state, Commonwealth and international law enforcement partners to exchange intelligence and disrupt organised crime.

“The diverse capabilities and skills across the AFP and our law enforcement partners strengthens our collaboration and effectiveness in tackling organised crime groups,” Commander Rice said.

“Criminals are driven by their own greed and profit. The harm caused by organised crime syndicates’ involvement in the Australian illicit drug trade is significant.”

ABF Commander David Coyles said that while the ABF had detected large volumes of illicit drugs entering Australia via air, mail and sea cargo streams over the past year, authorities were also seeing an increase in the use of drug mules.

“Transnational and serious organised crime groups are working as hard as ever to target the Australian community, using whatever means necessary to grow their profits and gain a greater foothold within this criminal trade,” he said.

Sexton, D. (2026). AFP highlights fame of “hide and seek” with drug smugglers. Retrieved from <https://www.thedcn.com.au/news/afp-highlights-game-of-hide-and-seek-with-drug-smugglers> on 22nd January, 2026.



## RETHINKING CARGOWISE AS COSTS RISE

**A**s freight forwarders absorb the impact of CargoWise's latest pricing changes, some are beginning to revisit an idea long considered impractical: building their own transport management system (TMS).

For most of the industry, the answer remains no. But for the largest global forwarders—where annual software costs are now approaching nine figures—the question is no longer purely theoretical.

"To compete with CargoWise, you're talking easily \$100m in investment capital," an industry professional said, "and that's just to get to where they are today." He added that replicating core functionality would take years, with customs systems presenting a particular challenge. "US customs would probably take you three years." More fundamentally, self-building a platform would require forwarders to radically rethink their operating model. That reality helps explain why, over the past decade, the industry has overwhelmingly outsourced its core systems. 13 of the world's top 25 global forwarders now operate on WiseTech's CargoWise One platform, including DSV, DHL, Ceva Logistics, Sinotrans and Nippon Express.

The industry's cautionary example remains DHL Global Forwarding's abandoned New Forwarding Environment project, which was publicly written off at €345m, with industry sources often suggesting the true cost was significantly higher. That episode helped cement CargoWise's position as the default enterprise TMS.

However, for a small group of global players, the sheer scale of current licensing costs is prompting renewed debate.

Off the record, several executives estimate DSV has been paying WiseTech between \$100m and \$150m annually for CargoWise. Bernstein analysts argued this week that following its acquisition of DB Schenker, DSV's size could make ending its long-standing relationship with WiseTech economically viable. Bernstein estimates DSV's CargoWise costs at around \$78m a year.

"That would pay for a lot of engineers to build it yourself," one executive said.

According to one source, building and maintaining an in-house system at that scale would cost a similar amount annually—between \$100m and \$150m—but with a crucial distinction: ownership. That ownership brings

control over pricing exposure, development priorities, data governance and upgrade timing—issues that have become increasingly sensitive as forwarders voice concerns about unilateral vendor changes.

Costs, however, vary widely depending on scale and complexity. One source estimated that a small forwarder could develop a basic system for a “couple of million”, while for a company the size of DHL, “it would cost the same as building a new CargoWise”.

Several sources noted that while CargoWise’s recent price increases have been steeper than before, they are not unprecedented. “WiseTech is playing a smart game,” one source said. “Forwarders depend on them, so they raised the price. They’ve done this every year – just much more aggressively this time.” One estimate suggests current pricing equates to roughly \$50 per transaction, covering origin, main carriage, destination and customs, excluding additional charges that customers say were not always transparent. “Software is expensive to build,” the source added. “So it’s not strange they’re charging for it now they have market power.” When combined with labour costs—often another

\$100 to \$200 per transaction—the impact on forwarding margins becomes increasingly material.

Other digital forwarders have attempted to pivot. Sources say the broader lesson is clear: building technology is one challenge, but turning it into a sustainable business is another. For small and mid-sized forwarders, self-building remains widely viewed as unrealistic, though alternatives are emerging. Ultimately, the real decision facing most operators is not whether to build or buy, but whether to optimise existing systems or seek an alternative vendor.

Lennane, A. (2026). CargoWise and the self-build question: when does a forwarder go it alone? Retrieved from <https://theloadstar.com/cargowise-and-the-self-build-question-when-does-a-forwarder-go-it-alone/> on 23rd January, 2026.



# STAFF SPOTLIGHT

## MARIANA GILL ADMIN/DISPATCHER TOMAX WAREHOUSING

### What is your role at Tomax?

Warehouse Admin and Despatcher.

### What do you enjoy doing in your free time?

I don't know what that is anymore? Hahaha!

### Do you have any plans for end of year/Christmas?

Camping with family. Our family loves to enjoy the nature and unwind from the hectic year!

### Favourite place to dine in Melbourne?

Anshumann. An Indian restaurant with great food! Highly recommend!

### Proudest achievement?

My 3 beautiful children.

### Name 3 things that instantly put a smile on your face?

Our newest addition Charlie, chocolate and of course, my kids.

### Your go-to karaoke song?

Anything from the 80's!!!

### What was your first ever job?

I worked in the head office at Dandenong Market.

