Continuum

WEEKLY RISK UPDATE / JUNE 19, 2026

Crypto Exploits, Crackdowns, and DeFi Capital Moves Into Coverage: This Week in Asia Risk

Swipe to read →

Continuum

01

REGULATORY

Japan moves to ban crypto insider trading as FIEA reclassification takes hold in 2026

Japan's Financial Services Agency, working with the Securities and Exchange Surveillance Commission, is implementing amendments to the Financial Instruments and Exchange Act that explicitly ban insider trading in cryptocurrencies. Under the framework, 105 digital assets including Bitcoin and Ethereum are being reclassified as financial instruments, making trading on non-public information a criminal offence subject to increased fines and prosecution, mirroring existing securities law. Japan's enforcement approach directly follows the MiCA model in Europe and South Korea's Digital Asset Basic Act and represents the most consequential regulatory shift for institutional crypto participants in the region this year. For insurers writing D&O and PI for crypto exchanges and digital asset platforms operating in Japan, this materially widens the scope of conduct risk.

→

REGULATORY

Singapore's June 30 DTSP deadline is now under two weeks away, with no grace period

Singapore's hard deadline for unlicensed Digital Token Service Providers serving overseas-only clients to either obtain a Part 9 FSMA license or cease operations is now eleven days away. MAS has been explicit: licenses will be granted only in extremely limited circumstances, and there is no transitional period. Firms that remain unlicensed after June 30 face forced wind-down. The rule targets platforms that use Singapore as an operational base while serving no local clients, which MAS views as a high money-laundering risk structure. For risk teams, the deadline is a live trigger: any counterparty, partner or investee with a Singapore DTSP structure should have confirmed their status by now.

HACKING & PHYSICAL RISKS

$127M stolen in cross-chain bridge attack targeting institutional market makers

A 12-minute assault beginning at 03:42 UTC on June 14 drained $127M from three DeFi protocols, BridgeLink ($52M), CrossFlow ($48M) and Relay Protocol ($27M), in what researchers describe as the largest bridge exploit since Wormhole's $325M breach in February. The attacker combined two vectors: compromising validator node SSH access via phishing to gain signing key control, then exploiting the bridge's acceptance of single-block confirmation rather than chain finality, allowing fraudulent cross-chain messages to authorize minting on destination chains before the source transaction was verifiable. Five institutional market makers, Wintermute, Jump Crypto, GSR, Amber Group and a fifth unnamed firm, suffered direct exposure totaling $57M in locked or unreconciled positions. Bridge governance token prices fell 18-31% within hours. As of June 16, roughly $89M remained in liquid form across chains, with $38M converted to privacy tokens. The attack traces a clear line to the Ronin ($198M, March) and Wormhole events: multi-month bridge attack campaigns targeting consensus logic rather than smart contract code, requiring institutional security standards insurers have not yet priced.

HACKING & PHYSICAL RISKS

DOJ-led "Disruption Week" freezes $3.8M tied to Southeast Asia scam compounds

The US Department of Justice's Scam Center Strike Force announced on June 3-4 that a coordinated operation with Coinbase, Meta, Microsoft, Apple, Google and SpaceX disrupted 1.4 million accounts and froze over $3.8M in cryptocurrency linked to pig-butchering and romance-baiting scam networks operating from Southeast Asian compounds. Thai police separately arrested 63 people connected to the operations. With global scam losses hitting $7.2B in 2025, the action underscores that Southeast Asia-based fraud infrastructure remains a persistent source of crypto-related loss and reputational risk for institutions whose platforms or rails get used as off-ramps, a relevant data point for crime and cyber policies covering payment processors and exchanges with regional exposure.

INDUSTRY & MARKETS

Coinbase Ventures backs onchain reinsurance protocol Re as real-world risk meets DeFi capital

Re, the onchain protocol operating under the Cover Re brand through a Cayman Islands licensed reinsurance vehicle, has secured a strategic investment from Coinbase Ventures to accelerate the tokenisation of reinsurance capital. The firm has written $500 million in premiums to date and expects to add $400 million in new business this year, targeting a $1 billion annual run rate by early 2027. Its flagship product, reUSD, is live on Base, Coinbase's Ethereum layer-2 network, and accepts USDC deposits. The model splits reinsurance exposure into on-chain tranches, giving a broader pool of investors yield derived from insurance premiums rather than leverage or token emissions. Coinbase Ventures' backing is a meaningful signal: it has concentrated recent activity on teams moving real-world assets and established businesses onto blockchain rails, and reinsurance, with its structured premium flows and regulated carriers, fits that thesis directly.

INSURANCE SPOTLIGHT

Willis: cyber cover delivers on most breach and first-party losses, but the gap is widening at the top

Willis published its Cyber Claims in Focus report on June 16, analysing 5,500 claims across 95 countries from 2013 to January 2026. The headline finding is that cyber insurance covered more than 95% of average data breach losses and over 90% of average first-party losses, providing genuine protection for the majority of insured events. The caveat is in the tail: a single ransomware event in the dataset surpassed $500M in losses, and the average ransomware claim now runs to $5.3M over 25 days. Keating's observation for Asia specifically is that limit adequacy is drawing increasing scrutiny from buyers, given this average severity. The report sits directly alongside the INTERPOL data as a complementary read: INTERPOL documents how severe and accelerating the threat environment is; Willis documents how the current insurance market is performing against it and where the coverage conversation needs to go next.

→

Continuum

Continuum helps Web3 companies and emerging tech meet their contractual, regulatory, and risk requirements — from liability, cyber, and crime to personal executive coverage."

Contact us to find the right coverage for your business.

www.continuuminsure.com