Credit Control Journal and Asset & Risk Review brings the most authoritative information to CEOs, CFO, and CIOs looking to improve business performance and create innovative, value-driven organizations.

Articles are written by experts whose authority comes from careful analysis, study, and experience, and are relevant to different industries, sectors and geographical locations.

Covering all areas of: Business Performance, Finance and Credit Analytics, Credit and Asset Management, Economics, Corporate Governance, Equities and Investments, Asset Funding and Insurance, Management Strategies, Corporate Purpose, Corporate Fraud, Law and Legislation, Environmental, Social and Governance (ESG), Innovation across all industry sectors including Pharmaceuticals and Life Sciences, IT and Software, AI and Emerging Technologies, Document Management Solutions, Cybersecurity.

The ideas presented in these articles have been tested in the real world of business and can be translated into action.

Cryptocurrency attacks rise, warns Invictus Risk Solutions

As cryptocurrency comes under attack by cyber criminals, we talk to Paul Rowland, Senior Partner, Invictus Risk Solutions for his views on the Lazarus Group's cyberattack on Bybit.

"At 215 pm on a Friday afternoon of the 21 March, the Pyongyang-linked North Korean team of notorious para-military hackers called the "Lazarus Group" took just two minutes to steal USD$1.5 billion in Ethereum cryptocurrency in a carefully planned and single biggest cryptocurrency cybersecurity breach and theft."

"Allegedly, the North Korean cyber agents, are tasked with stealing funds from the West and operate under the direction of Kim Jong-un's state military intelligence service, the Reconnaissance General Bureau.

“The cyber attackers compromised a ‘cold wallet’ encrypted and secure offline USB-stick used by the Dubai-based cryptocurrency exchange Bybit and drained 400,000 Ethereum cryptocurrency coins from the account.”

“A post-mortem forensic report commissioned by Bybit from cyber security experts Sygnia and Verichains concluded that when the Bybit cryptocurrency exchange attempted to move funds legitimately from their hardware wallet into an online account for an authorized client, the attackers were able to strike.”

“Within seconds, the group had breached the technology by piecing together the process from historical digital records and by activating an undetected backdoor malicious code that they had two days previously and secretly injected into the online Safe Wallet infrastructure. This enabled the group to activate their code to mimic and communicate directly with the coded signature of three Bybit accounts, including the Bybit CEO, Ben Zhou.”

“After the malicious transaction was executed, the hackers removed their code and escaped from the system before the Bybit security system even identified a breach and realised the currency was gone.”

“The company that designed and manufactured the cold wallet, Safe Global, said the hackers had managed to compromise the security by a combination of sophisticated social engineering, phishing attacks and technical brilliance to expose the system and override all instructions and protocols.”

“Safe Global has stated that its cold wallets have all been fully rebuilt with a reconfigured infrastructure that rotates all credentials to eliminate and prevent any future attack vectors.”

“The North Korean Group subsequently laundered all the funds through a series of legitimate cryptocurrency exchanges, converting the Ethereum to Bitcoin and other virtual assets and dispersing these across thousands of accounts on multiple blockchains to finance the country’s military and weapons of mass destruction.”

“The Bybit hack and theft represents the most devastating attack yet by the North Korean Lazarus Group and eclipses the USD$1.3 billion stolen by them over the whole of 2024.”

“The Lazarus Group has now been blamed by the FBI for a total of USD$6 billion in cryptocurrency thefts over the last decade. An FBI taskforce is actively trying to identify exchanges and block/capture/freeze suspect transactions.”

“Digital coin transactions are anonymous, and few exchanges follow KYC anti-fraud checks, with little incentive to comply with investigations in the unregulated space. However, most digital coin transactions can still be tracked through a deep internet dive via ledger blockchain technology, where a digital footprint can be identified and followed by cybersecurity experts.”