Brighton
You insure, We ensure

INSIGHTS

AUGUST/SEPTEMBER 2026



The Board Decision Hiding Inside Every D&O Claim

Beyond Bricks and Mortar

The Financial Reality of Modern Maritime Risk

Editor's Note

Dear Readers,

Across every sector, the boundary between the physical and digital worlds has dissolved. Risk is no longer an isolated event tied to a single asset or moment in time; it has evolved into a hyper-connected, multi-dimensional system. This issue explores a central theme reshaping modern risk management: The Interconnected Risk Ecosystem.

From AI-driven fraud at point-of-sale onboarding to board liability amid geopolitical volatility, and from smart building systems in Asia Pacific to automated marine port terminals, traditional boundaries are vanishing. Whether evaluating corporate governance, infrastructure commissioning, or global supply chains, modern vulnerabilities no longer stem solely from physical damage or immediate claims. Instead, they emerge from systemic dependencies, digital platforms, and the speed at which decisions are made and executed.

As these operational realities converge, risk leaders, underwriters, and directors must move beyond reactive frameworks. Managing exposure today demands holistic visibility, proactive governance, and an architectural approach to protection across interconnected platforms.

Ultimately, mastering this interconnected landscape is not merely about mitigating downside threat—it is about building the organisational resilience required to capitalise on growth with confidence. By anticipating systemic failures before they cascade, forward-thinking leaders can transform complex risk into a sustainable strategic advantage. We hope this edition offers valuable insights as you navigate this new era of complex risk.



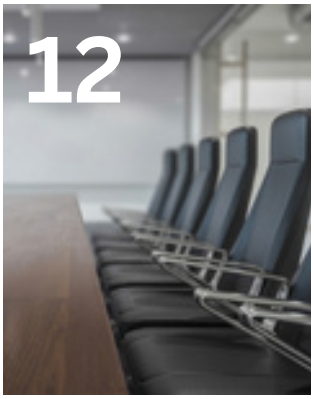
Annie Undikai

Annie Undikai, Managing Editor

Brighton
INSIGHTS
AUGUST/SEPTEMBER 2026

IN THIS ISSUE









02 Editor's Note

05 The New Architecture of Fraud Prevention
Fraudsters are now utilising counterfeit documents not only to exaggerate claims but also to gain access to the system. Insurers that evaluate each document as an isolated yes-or-no decision will continue to face losses.

12 The Board Decision Hiding Inside Every D&O Claim
Companies once reacted to geopolitical shocks such as conflicts and tariffs. Now the claims land on the board's own decisions, and on how honestly it explained them.

18 Beyond Bricks and Mortar
Rapid growth in hyper-connected commercial facilities across Asia Pacific is introducing advanced technology risks and compressed build schedules that redefine loss dynamics for Engineering All Risk underwriters and reinsurance brokers.

24 The Financial Reality of Modern Maritime Risk
The Baltimore bridge disaster showed how one marine incident can trigger widespread losses, highlighting the need for tailored marine insurance, stronger risk assessment and resilience-focused underwriting.



DRIVING SUCCESS

At Brighton, we provide exceptional solutions with cutting-edge software and dedicated support to advance your business in the competitive insurance industry.

TRUSTED STRENGTH

Rated **LECA1** by RAM Ratings, Brighton represents the pinnacle of capability and performance. We also stand at the forefront of global standards with successful compliance with **IFRS 17**.

EXCELLENCE ENSURED

You insure, we ensure — driving your future forward with confidence and exceptional performance.

OUR SOLUTIONS

- LICENSING & COMPLIANCE
- ACCOUNTING SERVICES
- WEBBIE, CLOUD-BASED ACCOUNTING SOFTWARE
- PAYROLL SERVICES
- GST/SST REPORTING
- E-INVOICING
- WORK PERMIT APPLICATION
- CORPORATE TAX SUBMISSION
- INTERNAL AUDIT
- SHARIAH ADVISORY
- COMPREHENSIVE CAPTIVE MANAGEMENT
- RUN-OFF MANAGEMENT
- SERVICED OFFICE FACILITIES

For more information, visit us at www.brighton.asia or scan the QR code



The New Architecture of Fraud Prevention

Picture a motor insurer that pays a claim for a rear-end collision. The photos are clean, the repair invoice is plausible, and the claims handler finds nothing wrong. Six months earlier, the same policyholder was accepted on the strength of a no-claims bonus letter that no previous insurer had ever issued. Nobody checked it carefully because speed and conversion were the primary priorities at the quote stage.

For years, insurers focused their document defenses primarily on the claims stage. Today, point-of-sale controls face equal pressure. The fraud did not start with the claim; it started at quote, and the claim was simply the eventual payout.

Official UK statistics document 684,800 blocked application fraud attempts, up 7.4% year-on-year, while major individual carriers report stopping more than 105,000 fake applications each year.

Meanwhile in the US, the Coalition Against Insurance Fraud has estimated that fraud accounts for roughly 10% of property-casualty losses, with total losses across all lines put at over $308.6 billion annually.

And when generative AI makes a convincing utility bill, bank statement, or ID a few minutes' work, the cheapest place to attack is the point where the insurer is least suspicious and most eager to say yes.

Fraudsters Are Moving Upstream

Three key forces are driving fraud towards the point of policy inception, where a single forged document can cause significant damage with minimal effort. Each of these factors makes quoting and onboarding more appealing targets than claims, and collectively, they highlight why payment controls alone are no longer sufficient.

The first is that forgery has become cheap. In Asia Pacific, the shift is stark. Research data indicates a 16.4% year-on-year rise in the regional fraud rate, along with a 142% surge in synthetic identity attacks.

Research data indicates a 16.4% year-on-year rise in the regional fraud rate, along with a 142% surge in synthetic identity attacks.

Malaysia is among the markets flagged as hotspots, alongside Pakistan, Indonesia and, the Philippines, because of rising digital adoption and insufficient regulation. Experts in this field indicate that AI has transitioned from merely a tool for creating fake IDs and altering documents to becoming part of a more advanced fraud production ecosystem.

The second is that quote stage has become a testing ground. A sophisticated fraudster doesn't commit to one insurer; they probe. Submitting a fabricated document at quote costs almost nothing, and if it passes, the insurer has revealed how strong its controls are further down the line. Think of it as reconnaissance with a purchase attached.

Finally, a policy that gets past screening becomes an asset in its own right. Once a policy is on the books, it carries a presumption of legitimacy, so later warning signs are more likely to be waved through.

Some fraudsters exploit this by choosing when to be scrutinised, timing a forged document so it gets its best chance of approval. After that, the insurer's own records vouch for it.

The unsettling reality is that a control failure at the outset does not remain confined to that moment. Instead, it establishes a precedent that undermines every subsequent control.



One Weakness, Three Tactics

These forces are not confined to one market. Three cases, from the UK, India, and Hong Kong and Singapore, show the same weakness exploited in three different ways: through doctored images, through intermediaries, and through impersonation.

In the UK, the tactic is the shallowfake: a real image, edited just enough to deceive. Allianz reported a 300% rise in incidents involving apps that alter images, videos and documents between 2021-22 and 2022-23.

In another incident, it was reported that fraudsters took pictures of written-off cars from salvage websites and altered the registration number, making the vehicle seem like the one being claimed.

Innocent people can be caught up too. In one LV= case, a man's photo of his work van, posted on his business social media page, was edited to show damage that never existed, and a claim was made in his name for an accident that never happened.

A similar fraud mechanism can operate through people rather than pixels. A case study from India, published by the General Insurance Council, describes a scheme where agents and diagnostic centres worked together to submit forged health check-up reports. The claim amount was then passed back to customers indirectly as a rebate on the policy.

In most cases, the customers weren't even aware of the claims. It was uncovered through field investigation: visiting labs and interviewing owners, staff, and agents. The lesson is that fraud at the point of sale can be perpetrated by intermediaries as easily as by AI.

Another example comes from Hong Kong and Singapore, where fraudsters used document fraud to divert corporate funds rather than target insurance claims, highlighting the evolving nature of document fraud.

In 2024, an employee in Hong Kong transferred US$25 million after deepfake technology was used to impersonate company executives during a video call. Similarly, in March 2025, a finance director in Singapore nearly lost over $499,000 in a near-identical Zoom-based attack.

Neither was an insurance fraud, but the same synthetic-identity playbook can be aimed at an onboarding portal.

The Trap of Single-Document Thinking

Most detection tools ask the same question: is this document real? That question is necessary but no longer sufficient, for two reasons.

First, detection is becoming increasingly uncertain. Research from Verisk found that people identify sophisticated AI-generated insurance images correctly only about 50% of the time, roughly no better than a coin toss.

The lesson is that fraud at the point of sale can be perpetrated by intermediaries as easily as by AI.

The same research reported that 99% of insurers have encountered AI-manipulated documents during claims handling, yet only 32% are highly confident in their ability to detect deepfakes.

That uncertainty becomes even more difficult to manage because not every suspicious-looking document is fraudulent. Legitimate documents can appear unusual for ordinary reasons, such as compression, scanning, or image enhancement.

Investigators who chase every anomaly risk wasting valuable time and delaying legitimate claims. Those who overlook genuine warning signs risk letting fraudulent claims through.

The gap between awareness and action is striking. In FRISS's 2026 survey of insurance fraud practitioners, 58% expect deepfakes to become the dominant fraud tool in the near term. Yet only 20% consider document and media verification a critical operational priority, while 9% report that it is not used at all. Many insurers see deepfakes coming, but far fewer are investing in the tools to detect them.

Second, detecting a single fraudulent document may not reveal the wider fraud. Organised fraud is rarely about one forged page. It often involves a pattern of activity across multiple applications.

The UK fraud-prevention body Cifas reported that its members are seeing AI-enabled document forgery and unregulated brokers acting as "application helpers", with some fake documents reused across multiple applications.

Cifas also cited that the number of insurance false-application cases fell by 30% from the unusually high levels recorded in 2024, while the number of insurance identity-fraud cases rose by 26%, exceeding 16,000 cases.

The nature of the problem is shifting from straightforward non-disclosure towards identity and document fraud, making patterns across applications increasingly important to detect. The better question is not "is this document fake?" but "what does this document tell me about the person, the network, and the timing behind it?"

A Practical Framework: Place, Pattern, People

Risk leaders looking to adapt do not need to rebuild everything at once. A more practical starting point is to organise their response around three ideas: where to check, how to read what they find, and who is doing the checking.

Place: Check where it matters most. Map the whole policy lifecycle, from onboarding through mid-term changes to renewal, and ask where a forged document would do the most damage for the least effort. Mid-term changes are often the weakest point because they feel routine, so they get less scrutiny than a new application.

Analysts in Asia Pacific argue that one-off, static checks are no longer enough. They recommend layered systems that assess risk signals in real time, at every stage where a document can change what the insurer is exposed to.

Pattern: Read each document in context. A single document rarely tells you much. What matters is what surrounds it. Look for the same document reused across applications, connections between the people and entities involved, and behaviour that doesn't fit a genuine customer. Sharing data is what makes this possible, because a customer who is new to your book may already be known to another insurer.



In Malaysia, an industry-wide database lets insurers confirm no-claims discounts and detect application fraud, while in South Korea, regulators are combining claims intelligence to identify suspicious patterns across health and motor lines.

People: Train the staff who see documents first. Contact centre and onboarding teams are part of the fraud defense, yet they are rarely trained as if they were. Fraudsters know these teams have far less forensic support than a dedicated investigations unit.

Give frontline staff a short list of red flags and a simple way to escalate a concern, and teach them that a helpful, cooperative customer is not automatically a trustworthy one. The same applies to distribution channel. As the Indian case showed, agents and intermediaries can be the ones submitting forged documents.

The Balancing Act

Security controls inevitably introduce operational trade-offs. Each extra validation step creates user friction, quietly eroding conversion, customer satisfaction, and brand trust. Rather than subjecting every user to heavy scrutiny, organisations must adopt a balanced, risk-based approach.

A successful fraud mitigation strategy should provide a seamless experience for low-risk transactions, escalate verification only when necessary, and quickly clear genuine customers. Strategies that alienate honest buyers, despite effectively capturing fraud, ultimately fail commercially.

Catching fraud late is costly, and more so in some markets. One Asia Pacific analysis cites benchmarks putting the cost of dealing with fraud at US$4.59 for every US$1 lost, higher than in the US or Europe.

A good test for any control is to ask two questions: how much fraud does it catch, and how many genuine customers does it wrongly flag? Leaders who track both will make better trade-offs than those who track only one.

The Bottom Line

AI did not invent document fraud; it simply democratised it and shifted the threat to onboarding. Insurers keeping their best defenses at the claims stage are guarding the exit while leaving the front door unlocked. Winning against modern fraud is less about buying another software tool and more about asking what a document is part of, rather than whether it is genuine.

THE BOARD DECISION HIDING INSIDE EVERY D&O CLAIM

Geopolitics used to be something companies simply reacted to: a war, a sanctions announcement, a tariff, arriving from outside with no input from the board. For directors and officers, it is increasingly something the board decides how to handle, and the claims now landing are testing exactly that decision

In February 2022, numerous companies declared their exit from Russia. Many characterised this decision as a principled stance in press releases and ESG reports aimed at investors and the public. However, a Yale study monitoring these announcements revealed that several companies discreetly maintained or even resumed certain aspects of their operations in Russia, all while their public statements remained unchanged.

Notice where the exposure truly lies. It's not about the war itself; rather, it's the gap between what the board announced and the actions taken by the company. A shareholder who invested based on that announcement may have a claim against those responsible, which is independent of whether the war was anticipated.

The emphasis is now on how accurately the board represents its own decisions. This distinction is becoming a crucial aspect of geopolitical risk within Directors and Officers (D&O) insurance. This trend is evident in almost every major market, extending beyond those closest to areas of conflict.

From a Specialist Concern To Boardroom Priority

For most of the industry's history, geopolitical exposure was primarily managed by a select group of specialists, including energy companies, aerospace firms, and those operating in a few unstable regions. However, this concern has now become mainstream.

This shift is merely due to an increasingly unstable world, although that plays a role. Rather, it is because geopolitical events have begun to resemble the very failures that D&O policies were designed to address: instances where a board misjudged a significant risk or failed to inform investors once it gained a clearer understanding.

The shift is evident in the way underwriters and directors assess threats. Geopolitical risk entered the global top seven risks facing directors for the first time in 2026, according to one major D&O liability survey.

Geopolitical risk entered the global top seven risks facing directors for the first time in 2026, according to one major D&O liability survey.

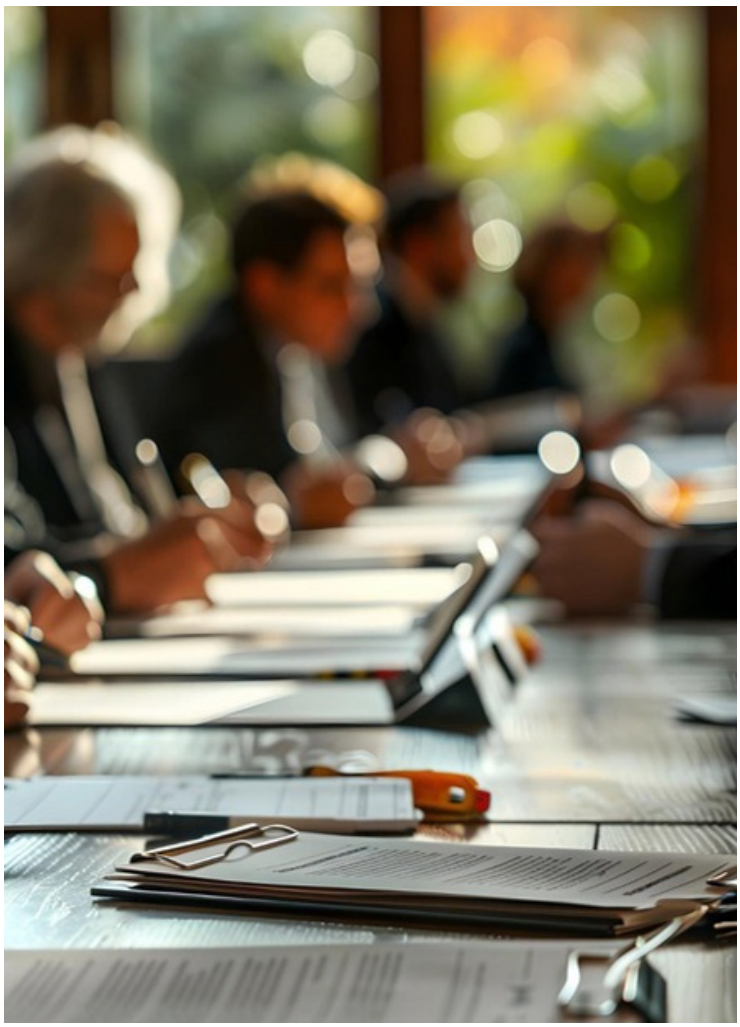
The regional breakdown shows why. In Europe, the ranking is even higher, coming in at sixth place. This is attributed to the region's close proximity to the conflict in Ukraine and its direct vulnerability to disruptions in energy supplies. Such concerns are already reflected in pricing. The industrial sector in Germany is experiencing increased premiums as insurers adjust their risk models in response to tariffs and trade barriers.

Asia exhibits a related yet distinct version of the same pressures, influenced more by the standoff between the US and China than by the war in Ukraine. In response to these tensions, Japan and South Korea are reassessing their insurance strategies to enhance domestic resilience.

Taiwan's crucial role in global technology supply chains makes it particularly vulnerable, given how deeply its semiconductor industry is tied to international trade. Regardless of the specific trigger, the core pattern remains unchanged. Boards are evaluated not on the instability itself, but on their ability to interpret it accurately and communicate their response transparently.

The nature of instability in global affairs has evolved. Previously, armed conflict was the main focus of geopolitical concerns within boardrooms. However, this has shifted to sanctions, tariffs, and trade controls as the leading sources of disruption. This shift is more significant than it may seem.

A war is an event that prompts a board's reaction. A sanctions regime, on the other hand, consists of regulations that a board must adhere to continuously across all jurisdictions, with updates on a schedule beyond their control.



Today's sanctions regimes are more extensive, detailed, and rigorously enforced than in the past. Furthermore, directors now face personal liability for violations, rather than just the company itself.

Companies are taking on these new risks at a time when their finances are already stretched thin. With insolvencies expected to rise for a fifth consecutive year, D&O liability is particularly heightened during and after bankruptcy proceedings. A board already under financial strain has little room to absorb a tariff shock or a sanctions misstep, and even less room to prove later that its decisions were reasonable given the information available at the time.

How Geopolitical D&O Risk Manifests

Geopolitics rarely appears in a claim by name. Instead, it shows up under familiar legal theories: disclosure failures, continuity lapses, and delayed strategic decisions.

Consider the securities class action filed against semiconductor supplier Photronics in July 2026. After missing its targets, the company's stock fell roughly 36% in a single day. Management pointed to macroeconomic uncertainty from the US-Iran conflict as a major cause.

Companies are taking on these new risks at a time when their finances are already stretched thin.

Shareholders did not file a lawsuit because Photronics was unable to foresee the conflict. Instead, they took legal action because management purportedly concealed internal operational slowdowns while still projecting robust growth, which ultimately led to disappointing results. The case makes the point better than any survey statistic: a board's own explanation for a bad quarter can become evidence against it if the underlying conditions were known internally before they were disclosed publicly.

Other claims centre on operational continuity. When early 2026 strikes on Iran drove up oil prices and disrupted Strait of Hormuz exports, operations absorbed the direct financial hit. However, board liability hinged on whether emergency plans were adequate and whether capital and supply chains were adapted quickly once the threat emerged.

In contrast, certain liabilities develop over time. Strategic choices to remain in a market, divest, or stay silent may seem defensible initially, but become indefensible as sanctions expand or hostilities escalate. Recent Russia divestment cases reflect this exact exposure pattern.

Underwriting Is One Step Behind

D&O underwriters have historically assessed geopolitical risk similarly to other tail risks, primarily by examining a company's physical asset locations. However, this approach is becoming less effective for a straightforward reason: a company without a physical presence in a sanctioned country can still face substantial exposure through a key customer, supplier, or banking partner.

Risk now flows seamlessly through commercial partners, just as it does across geographic borders. Therefore, an office map no longer accurately reflects where the actual exposure lies.

Risk also moves faster than standard underwriting cycles can handle. A sanctions list can change overnight, and a new tariff can be announced without warning. An annual renewal that reassesses geopolitical exposure once every twelve months is pricing a risk that has already shifted by the time the policy takes effect.

In response, underwriters are paying much closer attention to sanctions language, territorial definitions, and disclosure practices during initial underwriting, rather than treating geopolitics as background noise to address only when a claim occurs.

In the US, carriers are actively tightening war and sanctions exclusions in direct response to simultaneous conflicts across Europe, the Middle East, and Asia. This comes as directors face growing personal liability if a company fails to properly screen a transaction against an updated sanctions list.



What Boards and Insurers Can Do Differently

The clearest lesson from the Russia cases is that the greatest exposure rarely comes from the geopolitical event itself. Instead, it stems from the gap between a public statement and operational reality. Boards must treat every strategic or values-based announcement regarding geopolitical exposure as a disclosure that will eventually be tested, updating it promptly as facts change rather than leaving it unamended for years.

Both boards and insurers must identify exposure by examining commercial relationships instead of relying solely on physical addresses. The most significant risks often do not reside on a company's balance sheet. Instead, they typically flow through suppliers, customers, or financing partners that are several degrees removed —whether that connection leads to a sanctioned state or a Taiwanese chip supplier caught in the middle of two major economies.

Finally, underwriters require sanctions and continuity language precise enough to withstand a real event. Broad wording may seem efficient upfront, but it quickly fails when tested by a claim. Sanctions now sit at the very heart of underwriting, policy drafting, and claims handling alike.

The Cost of Silence

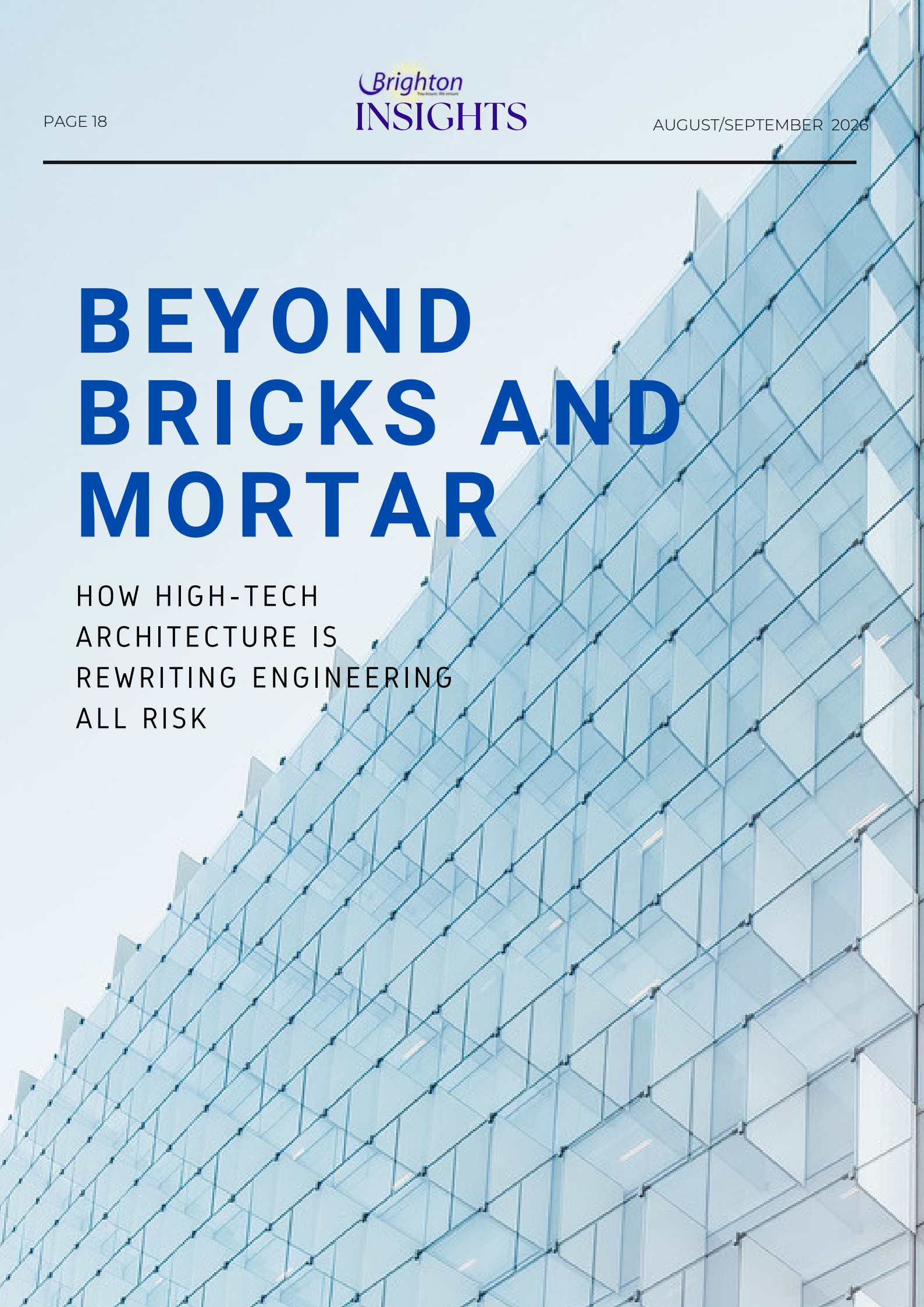
None of this comes without trade-offs. Closer governance scrutiny slows underwriting, and more detailed disclosures give activists and litigants more material to examine, not less. When facing a complex geopolitical crisis, a board's natural temptation is to manage the risk by saying as little as possible.

However, silence does not remove exposure. It only leaves the board without a record showing it acted reasonably with the information available at the time. Directors and their insurers fare best when clear, timely disclosure is treated as a line of defense rather than an added liability.

Geopolitics has transitioned from being a reactive concern for companies to a proactive element in decision-making. For D&O in markets like Germany, Japan, and South Korea, it now involves strategic choices about what to communicate and when. Companies are increasingly evaluated based on these decisions. Typically, claims arising from a war, tariffs, or sanctions do not hinge on the geopolitics itself; rather, they depend on whether the board's explanation of its actions stands firm when the facts come to light.

BEYOND BRICKS AND MORTAR

HOW HIGH-TECH ARCHITECTURE IS REWRITING ENGINEERING ALL RISK





The global construction skyline is undergoing a profound structural transformation, with Asia Pacific at the centre of this evolution. The traditional building blueprint, which is defined by heavy reinforced concrete, localised mechanical systems, and static electrical infrastructure, is giving way to hyper-connected, highly intelligent commercial ecosystems.

Regional market data indicates that Asia Pacific dominated the global smart building market, accounting for over 23% of revenue in 2025, driven by massive investments in smart cities, high-tech industrial hubs, and digital infrastructure across China, India, Japan, South Korea, and Southeast Asia.

Modern commercial assets, automated logistics centres, and specialised data facilities are no longer simple physical shelters. They function as dynamic computing platforms integrated with internet-of-things sensor networks, centralised building management platforms, energy micro-grids, and prefabricated modular units.

For underwriters, risk engineers, and reinsurance brokers negotiating Engineering All Risk and Contractors' All Risk policies, this technical leap introduces a fundamental paradigm shift. While smart building practices offer powerful tools to optimise site operations and prevent losses, they simultaneously compress project schedules, alter underlying risk profiles, and create complex loss dynamics that legacy policy wordings were never designed to absorb.

Reversal of the Construction Risk Curve

In conventional engineering insurance, property damage risks follow a well-understood chronological pattern. The highest potential for catastrophic physical loss historically sits during early civil works, foundation excavation, and core structural framing, where severe weather, flood, site collapse, and structural fires dominate claims. High-tech architecture effectively inverts this traditional exposure curve.

In smart construction projects throughout Asia, the most perilous and unpredictable phase arises as the project nears completion, particularly during final testing and commissioning. Industry analysis reveals that failures during testing and commissioning are becoming a larger portion of significant engineering losses associated with complex assets.

Modern intelligent facilities rely on intricate digital networks to maintain operational stability. Within these networks, building automation platforms, specialised liquid cooling loops, lithium-ion energy storage systems, and automated life-safety networks must function in seamless synchronisation.

A minor software glitch, dynamic configuration error, or sudden voltage fluctuation within a single digital controller can trigger a cascading failure across multiple interconnected systems.

Furthermore, expensive microprocessors, sensitive environmental sensors, and advanced climate control hardware are exceptionally vulnerable to micro-vibrations, dust contamination, and minor ambient temperature spikes long before formal project handover takes place.

The Convergence of Physical and Digital Exposures

The rapid adoption of smart construction methods blurs the operational boundary between physical project sites and cyber vulnerability. As contractors deploy operational technology, remote monitoring software, and temporary wireless networks during early site assembly, construction projects become increasingly vulnerable to digital threats.

The rapid adoption of smart construction methods blurs the operational boundary between physical project sites and cyber vulnerability.

A malware attack, ransomware event, or compromised network credential during the erection phase can lock project managers out of automated climate controls, halt environmental monitoring, or override temporary fire suppression setups.

Standard engineering policies traditionally feature broad cyber exclusions designed to separate property damage from purely digital losses. This creates significant friction and potential coverage disputes when a cyber incident or compromised software protocol directly causes physical damage, such as frozen cooling pipes, overheating electrical equipment, or unmonitored water leaks during construction.

Magnified Financial Fallout in Delay in Start-Up

High-tech construction projects generate immense revenue expectations that depend heavily on strict launch deadlines. If a physical or digital failure strikes during the fit-out phase, the financial fallout far exceeds the immediate repair costs. Recent market reports from major regional brokers like Aon Asia highlight that growing shortfalls in Delay in Start-Up recoveries pose a significant threat to project returns across Asia Pacific.

Replacing custom smart switchgear, specialised cooling chillers, or proprietary semiconductor controls involves long manufacturing lead times and complex global supply chains. Even a minor physical loss, such as water ingress spoiling low-voltage control wiring inside a service riser, can stall final testing and regulatory approval for months.

The resulting Delay in Start-Up claims, driven by ongoing debt service, developer penalties, and lost commercial revenue, frequently dwarf the direct property damage claim itself. In modern high-tech projects across fast-growing Asian commercial hubs, financial accumulation from time-element losses represents the single largest volatility factor for engineering underwriters and reinsurance treaties.



Supply Chain Interdependence and Modular Risks

The evolution of modern high-tech construction relies heavily on offsite prefabrication and advanced modular manufacturing. Complete plant rooms, pre-wired utility risers, and modular server enclosures are built in controlled factory environments across regional manufacturing hubs before being transported and installed on site. While this approach improves build quality and reduces site labour risks, it creates concentrated supply chain exposures for engineering underwriters.

Damage to just one offsite manufacturing facility or a transit incident involving specialised modular components can disrupt the entire construction timeline. Furthermore, pre-assembled digital components hold significant monetary value during offsite transit and storage, which transfers the risk burden to marine and transit endorsements linked to the main engineering policy.

Insurers need to thoroughly assess offsite accumulation, availability of components, and regional transit risks, along with site-specific hazards.

New Risk Prevention Standard

While advanced technology creates sophisticated underwriting challenges, it also equips insurers with unprecedented tools for loss prevention. High-tech job sites now deploy continuous telemetry that elevates risk quality and actively reduces claim frequency.

Industry data from corporate risk studies shows that implementing smart technology and internet-of-things monitoring platforms can reduce site operational energy waste and cut environmental damage incidents dramatically within the initial years of deployment.

Wireless moisture sensors positioned throughout internal pipe networks swiftly identify micro-leaks and activate automated shutoff valves, averting severe water damage during interior finishing. Machine-learning thermal cameras continuously monitor temporary power distribution boards and battery storage zones, detecting thermal anomalies well in advance of any potential electrical fires.

High-tech job sites now deploy continuous telemetry that elevates risk quality and actively reduces claim frequency.

Furthermore, real-time atmospheric sensors guarantee that sensitive digital infrastructure is unpacked and set up only when humidity and dust levels precisely match the manufacturer's specifications.

Updating the Underwriting and Brokerage Framework

Maintaining underwriting margins alongside modern smart construction requires insurers, risk engineers, and brokers to modernise their coverage structures. To begin with, policy wordings should separate basic mechanical testing from intricate digital integration testing, setting deductibles and limits that match longer commissioning timelines.

Additionally, underwriters should offer explicit rate discounts and better terms to project owners who mandate continuous site telemetry, including automated water shutoff valves and live thermal surveillance. Finally, insurers must address the cyber-physical gap by issuing clear endorsements that establish how policies respond when operational technology failures result in physical damage during construction.

Intelligent assets now define the global standard for modern construction, led by strong growth across Asia Pacific. As physical buildings become inextricably linked to their digital operating systems, engineering insurance must transition from a reactive claims payout tool into a proactive risk management partner.





THE FINANCIAL REALITY OF MODERN MARITIME RISK

In March 2024, the Port of Baltimore ground to a halt after the container ship Dali lost power three ship-lengths from the Francis Scott Key Bridge. The vessel struck a main support pier, collapsing the bridge, killing six construction workers, and completely closing the vital shipping channel.

Insurers had reserved for the loss early, at roughly $1.5 billion, a figure that shaped renewal pricing across the marine market through 2024 and into 2025. As legal, salvage and reconstruction costs continued to rise, the total insured loss exceeded $2.8 billion, marking it as the largest single marine insurance loss in history, surpassing that of the Costa Concordia.

Maryland ultimately settled its own claims against the ship's owner and operator for $2.25 billion and separately pursued the shipbuilder over a preventable design flaw.

A loose signal wire triggered the physical crash, but the financial fallout revealed a structural flaw. Modern port risk has far outpaced legacy legal and insurance architectures. Citing an 1851 statute built for sailing ships, the owner of the Dali sought to limit liability to its post-casualty value of $43.7 million, a figure covering only a small fraction of total damages. This vast gulf between outdated legal assumptions and modern commercial losses illustrates a growing vulnerability across global shipping hubs.

Risk Profile Outruns Policy Wording

Modern port exposures have expanded beyond traditional physical asset schedules. Terminals now operate as intermodal hubs, directing rail, road, and sea traffic through software systems built long after legacy policy wordings were drafted. Automation spans entire container yards, placing software at the core of vessel and cargo management.

Consequently, operational continuity has become the primary driver of financial loss, easily overshadowing the physical destruction that initiates an event.

Global maritime cyber incidents surged by 103% year-on-year, climbing from 408 recorded events in 2024 to 828 in 2025, according to the 2026 Maritime Cyber Threat White Paper. Driven as much by geopolitical aggression as by criminal greed, this threat landscape is shifting rapidly beyond standard corporate data breaches toward core operational technology.

Modern port risk has far outpaced legacy legal and insurance architectures.

Threat actors now actively target satellite links, navigation gateways, shipboard maintenance systems, and automated terminal software, often encrypting critical voyage logs and port databases to demand hefty ransoms. A stark example occurred when Italy's Port of Ancona suffered a ransomware attack that laid bare its digital exposure.

Regardless of how deeply core networks were encrypted, the incident proved that a port's digital infrastructure is as vulnerable as its physical piers, and a digital outage can freeze cargo operations just as effectively as a major ship collision.

Regulatory bodies are moving far faster than standard policy wording can adapt. The International Maritime Organization introduced updated cyber risk guidelines in 2025, while mandatory classification requirements for vessel cyber resilience applied to newbuild contracts starting in mid-2024.

These regulatory shifts are far more than compliance updates. They are actively redefining what foundational concepts like seaworthy and operational mean for modern maritime assets, setting a new legal and technical benchmark that underwriters can no longer ignore.

Why Capacity Isn't Enough

For years, the marine and port market competed primarily on capacity by offering higher limits at lower prices. The Baltimore disaster shows why that approach solves the wrong problem. The policy behind the Dali had plenty of capacity, but it lacked a structure designed for multi-layered disruption that could affect a port, a state government, and a shipbuilder's liability at the same time.

During renewals, Protection and Indemnity insurers had to decide whether even a $3.1 billion reinsurance program was enough when a single bridge collision could exhaust it.



This principle applies equally to non-catastrophic events. A ransomware strike on a regional terminal, a software glitch at an automated yard, or a cascading delay across an intermodal rail link does not need to dominate global news to overwhelm a poorly designed policy.

Each of these events shares a common driver. The financial impact stems less from physical damage and more from prolonged downtime and the web of dependent businesses affected while operations remain stalled. This reality gives brokers and underwriters a clear strategic advantage.



Success now lies in analysing a port's true operational profile, including its automation tier, rail dependencies, and digital footprint, and crafting a policy tailored to those specific realities rather than simply selling higher limits on a generic form. A fully automated container hub and a traditional break-bulk port operate on entirely different risk curves, even if their insured physical values appear identical on paper.

Understand, Structure, Continuity

Effective coverage begins with evaluating a port's current risk profile rather than outdated renewal data. This requires mapping digital networks and automation frameworks alongside physical assets to pinpoint single points of failure. In Baltimore, a single electrical failure set off a chain of financial consequences that reached a port, a state, and a shipbuilder.

Policy structures must mirror these operational realities instead of relying on standard market wordings. Automated terminals need business interruption policies that trigger on system failures without requiring physical damage. Key terms, waiting periods, and sub-limits should be calibrated directly against a facility's real-world failure modes.

Crucially, underwriters must evaluate operational resilience alongside financial limits. Just as cyber underwriters audit response plans before binding coverage, port underwriters must assess how quickly a terminal can reroute traffic or reboot critical systems, matching policy timelines to actual recovery capabilities.

Tailored coverage requires significant investment from both brokers and underwriters. Designing a bespoke policy demands far more underwriting time than using a standard form, and brokers who compete on structure rather than price must understand a client's operation inside out.

In the wake of major events like Baltimore, insurers often face the temptation to cut capacity across the board rather than reprice the specific risks that caused the loss. While blanket capacity cuts protect balance sheets in the short term, they leave the underlying policy flaws completely unaddressed.

The more effective approach is less sensational but significantly more resilient. Insurers and brokers should build relationships based on a facility's genuine risk profile well in advance of any disasters, ensuring that the policy structure is solid when challenges arise.

The Bottom Line

The Dali loss was not a case of missing cover. The cover assumed a simpler port than the one that existed: less automated, less digitally interconnected, and less exposed to cascading failures across multiple parties.

The future of port insurance will rely less on the raw capacity a syndicate can deploy and far more on its technical understanding of a facility's unique operations and how those systems actually break.

