Beneath the Asset

Cyber Risk and the Infrastructure Institutions Depend On

A cybersecurity perspective on asset safety

Thomas Murray

Risk Intelligence | Due Diligence | Cyber Security

Foreword

When Thomas Murray published *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1), the argument was that asset safety had quietly stopped being a custody question and instead become an infrastructure question. CSDs, custodians, settlement systems, market access arrangements and the technology providers behind them now determine whether an institution's assets are safe, not just where those assets are legally held.

Cyber is no longer a discrete operational risk sitting alongside custody risk, settlement risk and geopolitical risk. It is now the mechanism through which those other risks most often materialise. A weak link at a technology provider, an IT outsourcer or a help desk is increasingly how the infrastructure beneath an asset fails.

The next disruption to reach an institution's assets may not begin with a bad trade, a downgraded counterparty or a market shock. Increasingly, it begins in a system, a supplier or a piece of infrastructure the institution never directly touches and finds out about only once it has already failed.

Executive summary

A flurry of events in 2025 and 2026 has shown the direct impact that technology outages and cyber threat actors can have on financial institutions, and in some cases impacting the wider market, for example the Japanese Securities Account Hijacking Campaign in 2025 (2). As of July 2026, the European Systemic Risk Board announced that frontier AI models from a cybersecurity perspective are a growing systemic risk for the European Financial Services sector (3). The paper states that “should incidents propagate through payment systems, clearing and settlement or other operational bottlenecks, they could severely disrupt or shock the financial system, undermine public confidence and lead to heightened financial volatility” (3). The risk is real.

The attack on Jaguar Land Rover was modelled at £1.9 billion in UK economic loss (4), the most damaging cyber event on record. The breach at Marks & Spencer cost roughly £300 million in lost profit (5). In both, the point of failure was a third party and a person, not the target’s own perimeter. The same pattern Thomas Murray’s flagship report (1) identified running through custody chains, CSDs and post-trade infrastructure.

This paper sets out how a failure of a third-party and human error extends the flagship reports (1) findings:

- Cyber risk is now the primary transmission mechanism for infrastructure risk. When a CSD, custodian, fund administrator or their outsourced providers are compromised, the assets sitting on that infrastructure are compromised with them.
- The exposure that matters most sits outside the institution’s own perimeter, in custodian sub-networks, IT outsourcers, cloud platforms and help desks, echoing the third party dependency finding from the flagship report (1).
- Geopolitics and cyber risk are converging. State-sponsored activity is now targeting the infrastructure layer directly, adding a further transmission path alongside the sanctions and market-access exposure. As shown recently in Iran in both June 2025 and June 2026 where destructive activity against Bank Sepah was reported with further cyber disruption at four major banks and later card-based banking services at three lenders (6).
- The tools institutions use to assess this risk today force a false choice: rich, one-entity-at-a-time due diligence, or broad but contextless surface scanning. Neither, alone, gives an asset owner or custodian a defensible, continuous view across a portfolio of dependencies.
- As with the rest of the *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1) thesis, the answer is not more due diligence done the same way, more often. It is continuous, contextualised risk intelligence across the full chain of infrastructure an institution’s assets depend on.

1. Asset safety, revisited through a cyber lens

Thomas Murray argued that the question institutions ask about their assets: where are they held, who is responsible for them, how strong are the controls around custody and settlement, is no longer sufficient on its own. Asset safety now depends on a wider chain: CSDs, custodians, clearing and settlement systems, technology providers and the third parties behind all of them.

Cyber risk is why that chain now matters as much as it does. All institution's assets are created, moved, recorded and defended through technology, and increasingly through technology operated by someone else; a sub-custodian's IT provider, a CSD's cloud platform, a fund administrator's outsourced help desk. When that technology is compromised, the asset is compromised with it. When the third party running it is compromised, the asset is compromised through it. The news that Accenture has suffered an incident highlight (7) the possibility that even the largest and critical third parties (as designated under DORA (8)) can fall victim to attacks and impact an extensive ecosystem of customers and clients.

Cyber risk as the specific route through which the infrastructure risk reaches an institution's assets.

2. Three forces widening the exposure

2.1 Digitalisation of post-trade infrastructure

The infrastructure beneath the asset is itself becoming more digital, and AI adoption is accelerating that shift. Back in 2025, an estimated eighty-eight percent of companies used AI in at least one business function (9), and “free AI” was the second most-searched AI term in the UK (10), a signal that much of the initial adoption could have been happening outside governed, sanctioned channels. Growing calls for further digitalisation of the industry have continued into 2026 with the UK government seeking to develop a framework for tokenisation of wholescale financial markets (11).

The modern technology providers have been targeted, including the Bybit crypto exchange heist which shows the potential for high-impact attacks on digital asset organisations. The attack resulted in an estimated $1.5 billion of assets stolen (12). For CSDs, custodians and their providers, this widens the surface through which an institution’s assets are exposed, often faster than governance can keep pace. Every new integration between a custodian and a technology vendor, every new AI tool adopted inside a sub-custodian’s operations, is a new dependency an asset owner cannot see and did not sign off.

2.2 A professionalised, AI-enabled threat landscape

Beneath the Asset: The New Infrastructure Risk in Global Markets (1) identified geopolitical shocks as a transmission path into custody chains. That path is now also a cyber one. A 2025 advisory from US CISA and international partners set out how state-sponsored actors have compromised networks worldwide, including telecommunications and critical infrastructure, to feed a global espionage system (13). Financial market infrastructure sits squarely inside that target set.

Social engineering, the method behind the M&S breach, has also been industrialised. ENISA’s 2025 threat landscape assessment found that by early 2025, AI-supported phishing campaigns represented more than eighty percent of observed social engineering activity worldwide (14). Ransomware, meanwhile, remains a mature and profitable criminal industry, with victim counts rising steadily since 2023 (15).

The result is an adversary well-resourced enough, and now automated enough, to probe every custodian, CSD, fund administrator and outsourcer in an institution’s chain, continuously, for the weakest point.

2.3 Perimeter expansion through the custody chain

The third force is the one that connects directly to Thomas Murray’s core argument (1). An institution’s cyber perimeter no longer ends at its own firewall; it extends through every custodian, sub-custodian, CSD, IT outsourcer and cloud platform in its custody and settlement chain. Even spanning into the very technology infrastructure that is needed to deliver modern banking services, as shown by the Telstra outage that impacted Australian payment systems earlier this month (16).

Even the ECB T2 payment system has had outages, highlighting the extension of the perimeter (17). Banks, FMIs and major payment participants must understand how firms manage queues, liquidity, cut-off times, client communications, contingency procedures and downstream settlement dependencies. The challenge is extensive and dependent on third parties.

The safety of an institution’s assets is now a function of the security of entities it does not control and, in most cases, cannot see. Cyber risk is simply the mechanism that turns an invisible dependency into a realised loss. Not only will individual first victims be the sole barer of loss, but due to the interconnected nature of the banking system, the impact could be extensive, and “could propagate across the broader financial system through payment systems, clearing and settlement, or other operational bottlenecks, and could originate both within and outside the EU.” (3)

3. When the risk materialises: JLR and M&S

Neither incident occurred inside financial market infrastructure, but both show, in sharp and quantified form, exactly the failure mode *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1) warned CSDs, custodians and asset owners to watch for: the loss did not come through the target's own front door.

3.1 Jaguar Land Rover: when infrastructure failure becomes a balance-sheet event

In late August 2025, an attack on JLR's internal IT environment halted global manufacturing for five to six weeks, idling major UK plants and rippling through a tightly coupled supplier base.

- **£1.9bn** modelled UK economic loss (range £1.6–£2.1bn), the most damaging UK cyber event on record (4)
- **5,000+** UK organisations affected; classed a Category 3 systemic event by the Cyber Monitoring Centre (4)

Losses ran at an estimated £50 million a week. The UK government underwrote a loan guarantee of up to £1.5 billion to keep suppliers' solvent, and the Bank of England later cited the disruption as a drag on third-quarter GDP (18).

The asset lost was operational capacity, and through it, enterprise and supply-chain value. JLR outsourced significant IT management to a third party, and the loss ran outward through that dependency, exactly the portfolio-of-connected-entities exposure that CSDs, custodians and their institutional clients carry through their own outsourcing and sub-custody chains.

3.2 Marks & Spencer: when the front door belongs to someone else

In April 2025, M&S suffered a ransomware incident that paused online orders for around 46 days and led to the theft of customer data. The company put the profit impact at roughly £300 million, with separate response and recovery costs of around £130 million (5).

Initial access did not come from breaking M&S's own defences. Attackers used social engineering against a third party run IT help desk, impersonating staff to obtain a password reset, then moved laterally and deployed ransomware.

Knowing who holds privileged access to an institution's systems, and through which third party, mattered more than the hardness of the perimeter. For a custodian or CSD, the equivalent exposure sits in outsourced service desks, sub-custodian relationships and technology vendors holding privileged access, exactly the class of dependency that annual due diligence questionnaires struggle to see, because the relationship itself, not a technical flaw, is the exposure.

The common thread

In both cases, attackers reached the crown-jewel asset through a third party and a person, not a technical exploit of the victim's own systems. That is the same pathway *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1) identified running through custody chains, cyber risk simply gives that pathway a name and a mechanism.

4. The assessment gap: why current tools cannot see this exposure at portfolio scale

Thomas Murray's fifth finding (1) was that banks and asset owners need live risk intelligence, not annual due diligence alone. Cyber risk is where that gap is most acute.

Two approaches dominate cyber risk assessment today, and each solves only half the problem for an institution trying to assure its full chain of custodians, CSDs and sub-custodians:

- **Maturity and control assessments**, deep, questionnaire-and-evidence reviews of a single custodian or provider, produce rich risk context but are point-in-time, hard to compare across a panel of custodians, and do not scale across a global chain of dependencies.
- **External attack-surface tools** scan the internet-facing footprint of many entities continuously but carry no risk context. They can show a port is open at a sub-custodian; they cannot say whether that matters to the assets sitting on that custodian's infrastructure, or whether it could withstand and recover from an attack.

	Maturity and control assessments	External attack-surface tools	Context-at-scale
Risk context	High	None	High
Portfolio scale (across a custody/ CSD panel)	Limited	High	High
Continuity	Point-in-time	Continuous	Continuous
Comparability across providers	Limited	Medium	High
	Rich context, one custodian at a time	Scale and continuity, without risk context	Risk context and portfolio scale, in one signal

For an asset owner or bank with a panel of custodians, sub-custodians and CSDs, neither approach alone can answer the question that matters: which of the entities my assets depend on are exposed, how badly, and could they withstand and recover from an incident?

5. A context-at-scale approach to the custody and settlement chain

The way out is not to choose between depth and breadth, but to combine them: contextualised risk signals across an entire panel of custodians, CSDs and their providers, refreshed continuously and comparable across entities.

This is the natural extension of the flagship report's (1) methodology point, that Thomas Murray's assessments of CSDs, custodians and post-trade infrastructure, built over more than three decades, are now being extended through cyber resilience ratings and continuous market intelligence. Giving institutions a single, ongoing view of the infrastructure beneath their assets rather than a point-in-time snapshot of one link in the chain.

For asset safety, that is the decisive shift. It lets a bank or asset owner see, at any moment, which custodians, CSDs and providers in its chain are exposed, how badly, and how they compare with peers, and to act before that exposure becomes a JLR- or M&S-scale loss. Both incidents were failures of visibility at the edges of the organisation, not failures of effort. Continuous, contextualised intelligence is designed to close exactly that gap.

6. What continuous context enables for institutional investors, banks and custodians

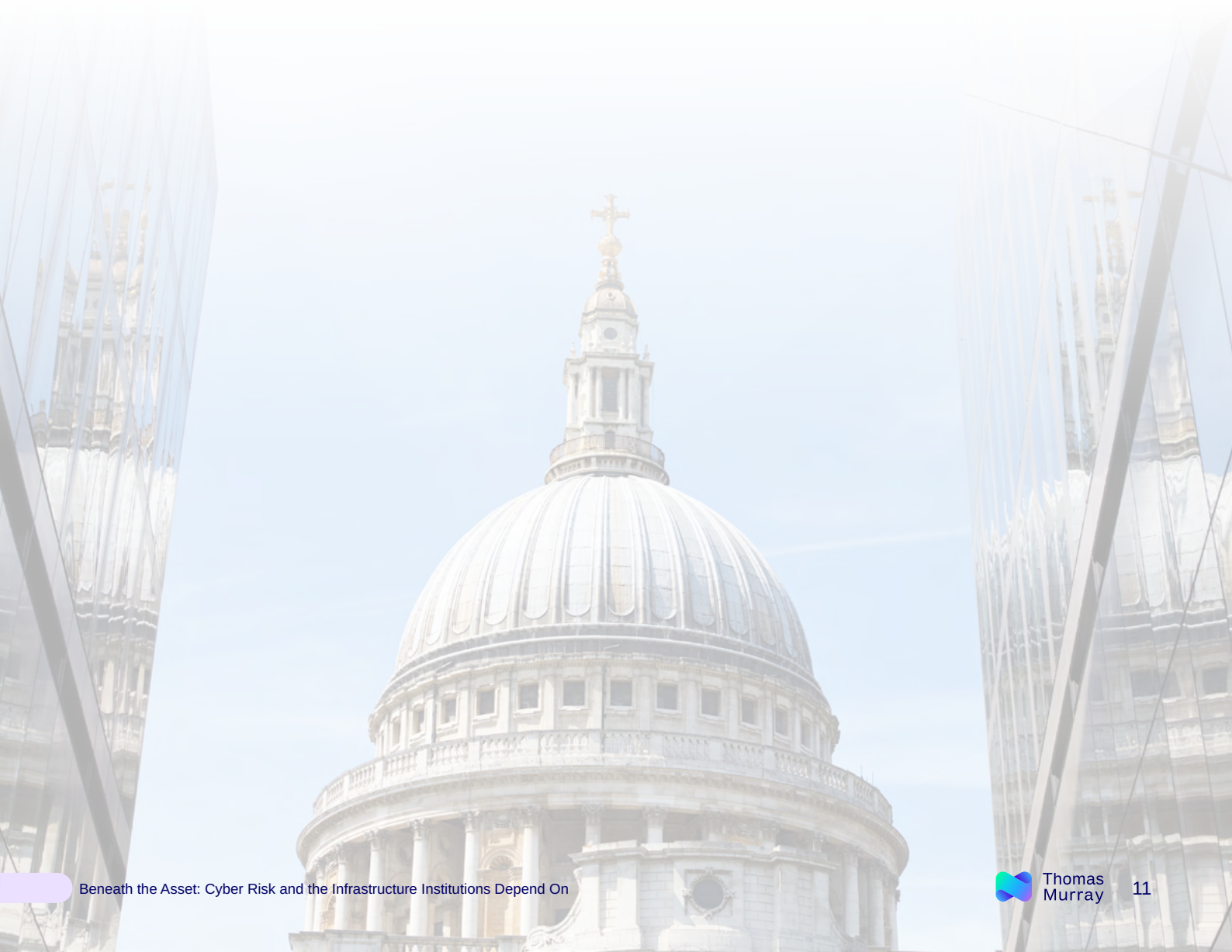
- **Nuanced risk positions, not a pass/fail score.** A graded view of where asset safety is genuinely at risk across a custody panel supports better, faster prioritisation than a binary due diligence outcome.
- **Resilience, not just security.** The question shifts from “is this custodian secure today?” to “if it is hit, can it respond, financially and technically, well enough that my assets survive?” That is the asset-safety question *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1) posed, and continuous cyber context is what makes it answerable
- **Defensible, continuous assurance.** Comparable signals across a custody and settlement chain, refreshed over time, replace one-off due diligence snapshots with an ongoing line of sight over the exposures that matter to institutional clients and regulators alike.

Thomas Murray is taking this thinking forward with a small group of like-minded organisations on a pathfinder programme, with further insights to follow.

7. Conclusion

Thomas Murray argued that the safety of an institution's assets now depends on a chain of infrastructure it does not fully control (1). This paper has shown the mechanism through which that dependency turns into loss: cyber risk, transmitted through third parties and people, reaching crown-jewel assets without ever touching the victim's own front door.

The institutions that keep their assets safe will be those that extend the logic of *Beneath the Asset: The New Infrastructure Risk in Global Markets* (1) into cyber specifically, treating their custodians, CSDs and outsourced providers not as a periodic, one-entity-at-a-time compliance exercise, but as a portfolio to be seen, in context, at scale and continuously.



References

(1) Beneath the Asset: The New Infrastructure Risk in Global Markets

(2) Financial Services Agency: Press Conference by KATO Katsunobu, Minister of Finance and Minister of State for Financial Services

(3) European Systemic Risk Board

(4) Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident - October 2025

(5) Marks & Spencer. 2025/26 results and disclosures; UK Parliament testimony on the April 2025 incident.

(6) Suspected Israeli hackers claim to destroy data at Iran's Bank Sepah

(7) Accenture confirms breach after hacker offers stolen data for sale

(8) Digital Operational Resilience Act

(9) Mckinsey, The state of AI in 2025: Agents, innovation, and transformation, 2025.

(10) Google Trends. UK search interest in "AI" and related queries, 2020–2025.

(11) Wholesale Digital Markets Champion- First Report

(12) Bybit Heist Case Study: When Billions Vanish

(13) US CISA and international partners. Joint advisory on state-sponsored actors compromising networks worldwide, 2025.

(14) Reading The Enisa Threat Landscape 2025 Report

(15) Ransomware.live. Cumulative ransomware victims by month, 2023–2026.

(16) Telstra Outage in Australia Disrupt Trains and Payments; No Evidence of 'Malicious' Activity

(17) ECB Payment System Suffers Second Outage in a Week

(18) Monetary Policy Report - November 2025

Contact us

Please get in touch to find out how we can help you to mitigate changing risk.

Find out more: thomasmurray.com
Contact: enquiries@thomasmurray.com

About us

Thomas Murray provides risk intelligence and ratings covering central securities depositories, custodians, market infrastructures and financial systems worldwide. For more than three decades, the firm has helped financial institutions understand and manage the risks affecting the safety, resilience and performance of their assets across global markets.