The Unpriced Catastrophe

How data breaches evaporate enterprise value and societal trust.

The criminals who breached Medibank, Australia's largest health insurer, in October 2022 understood something about corporate value that much of accounting still struggles to recognise. They demanded one dollar for each of the 9.7 million Australians whose records they had stolen, and when the insurer refused to pay, they published intensely personal medical information, including records relating to abortions and addiction treatment, on the dark web. Medibank initially put the direct cost at between $25 million and $35 million, excluding litigation and regulatory consequences, and Australia's prudential regulator later imposed an additional $250 million capital requirement over the weaknesses the breach exposed. These were significant penalties, yet neither captured the asset the attackers were truly targeting. They were attacking trust.

Boards, regulators and investors have been conditioned to see cyber risk through costs that accountants, lawyers and insurers can quantify: remediation, penalties, class actions and premiums. Those costs dominate breach reporting because they can be measured, provisioned and closed. The deeper loss behaves differently. When a customer loses trust, they quietly take their business elsewhere. When a citizen becomes reluctant to share information with government, no loss is recorded. When a business partner awards its next

contract to a competitor, the balance sheet remains unchanged. Yet in each case, something of real economic value has been destroyed.

That silence is the defining accounting problem of the digital economy. In 1975, tangible assets represented 83 per cent of the market value of the S&P 500; by the end of 2025, Ocean Tomo's fifty-year study put the intangible share at 92 per cent, a pattern the study finds repeated across global markets. Value has migrated from things organisations own to relationships people choose, and accounting has only partially followed, because IAS 38 generally prevents companies from recognising internally generated brands and customer relationships as assets. A company can estimate to the dollar the depreciation of a building yet cannot measure the deterioration of the confidence on which its digital business model depends. Call this the invisible balance sheet - the accumulated confidence that customers, employees, investors and governments place in an institution. That confidence is economic capital: it determines whether customers share data, investors allocate funds and citizens adopt digital services. In the digital economy, trust performs productive work.

Cybercriminals appear to understand this more clearly than many boards. IBM's 2026 Cost of a Data Breach Report found ransomware involved in 39 per cent of breaches, and in 41 per cent of those incidents the attackers' pressure point was brand reputation. Cyber extortion once centred on denying access to systems; increasingly the pressure comes from holding information whose disclosure would damage the relationship between an institution and the people who entrusted it. The ransom is now demanded against confidence rather than infrastructure, and the decisive question after a breach has shifted from what the regulator will fine to what customers will think when they discover what the organisation failed to protect. The same research explains why: 58 per cent of breached organisations had yet to rebuild customer trust, and nearly one in five needed more than 150 days to recover after containment. Servers can be restored, credentials reset and portions of the loss reimbursed. Trust has no backup.

> Resilience in the AI era will be defined less by preventing every intrusion than by ensuring successful intrusions yield progressively less value.

Artificial intelligence makes the problem urgent because it is dismantling a structural advantage defenders held for decades. IBM found that one in four malicious breaches were AI-enabled, a 56 per cent increase in a year, and Microsoft warns that frontier AI is dramatically accelerating vulnerability discovery. Cyber defence is becoming a contest between human defenders and machine-assisted adversaries operating at a speed no workforce can match. The perimeter is becoming more legible to the attacker while much of what sits behind it remains poorly protected: only 37 per cent of breached organisations

encrypted sensitive data both at rest and in transit, and just 34 per cent had visibility into their cryptographic assets. Each successful exfiltration transforms a technical vulnerability into a reputational weapon, and every breach becomes an attack on the invisible balance sheet.

Cyber doctrine must shift accordingly: resilience in the AI era will be defined less by preventing every intrusion than by ensuring successful intrusions yield progressively less value. Organisations must keep strengthening their perimeters while making critical information secure in its own right: discovered, classified, encrypted and protected throughout its lifecycle, with boards knowing where sensitive data resides, who can reach it and who holds the cryptographic keys. When attackers penetrate the perimeter, what they steal should be increasingly incapable of harming the institution behind it.

At national scale the same erosion becomes strategic. In the United States alone, the Identity Theft Resource Center counted 3,158 data compromises in 2024 and 1.7 billion victim notices, a rise of 312 per cent. Each incident is administered as an isolated failure; collectively they deplete society's willingness to trust institutions with information, and almost every economic transformation depends on that willingness, from digital identity schemes in Europe and India to AI-enabled healthcare and open banking. Without trust, digitisation slows; without digitisation, productivity slows; without productivity, national competitiveness weakens. Industrial-era strength rested on factories, ports and energy systems; digital-era strength rests on society's confident participation in trusted information systems. Every major breach imposes a small tax on digital adoption, and those taxes compound. Hostile states benefit from the cumulative effect without conducting every attack. Trust has become strategic infrastructure, and the nations that preserve it will digitise faster, deploy AI more effectively and create greater value from information than those that lose it.

Boards therefore need to rethink what they are protecting. Compliance establishes a floor rather than the value at risk; insurance can reimburse money, not confidence; and no organisation should assume permanent immunity from AI-enabled adversaries. The larger task is to treat trust as capital: measure customer confidence, retention, complaints and post-incident behaviour with the seriousness applied to financial risks, test how major data losses would move stakeholder confidence and enterprise value, and accelerate enterprise-wide data protection so the failure of one security layer does not expose the relationships on which the organisation depends.

The industrial age forced accounting to recognise that physical assets were being consumed even when bookkeeping could not observe the process; depreciation emerged because ignoring the erosion distorted the understanding of value. The AI age presents the equivalent challenge, and the accounts have yet to answer it: institutions can estimate the financial cost of a cyber incident to the nearest dollar yet cannot record the erosion of confidence that follows. Cyber resilience has

ceased to be a technology issue or compliance obligation; it has become a mechanism for preserving economic value and, increasingly, national power. The fine is visible, the remediation bill is visible, the insurance premium is visible. The customer who quietly decides never to trust you again is not. That is the liability on the invisible balance sheet, and in the AI age it may prove the most consequential cyber cost of all.