A soft market with a hard truth

State of Cyber: H1 2026

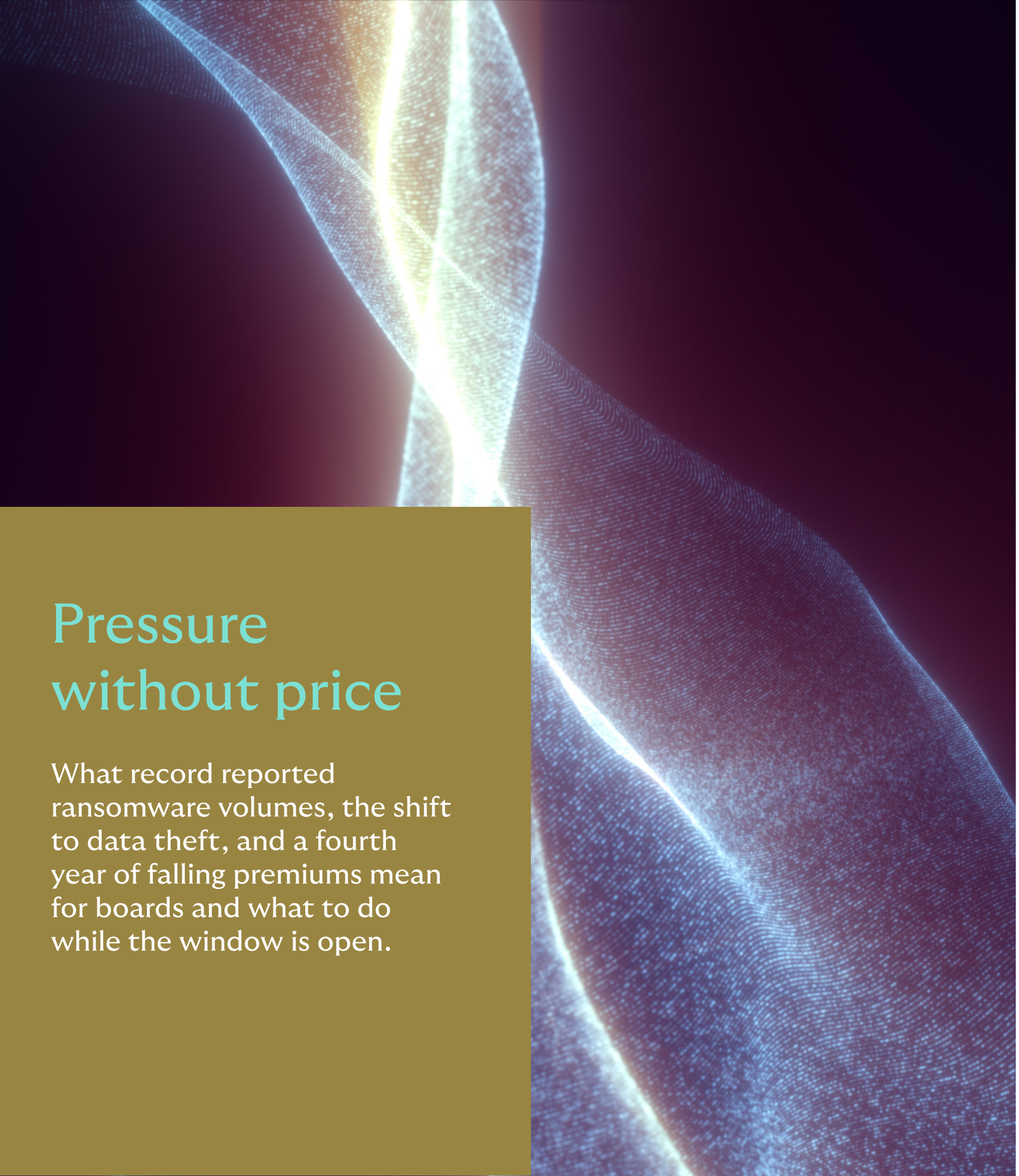
Pacific region

July 2026

Reporting period: 1 January - 30 June 2026

Classification: TLP CLEAR/Public

HOWDEN | NSB Cyber *No Steps Backward* | WK WOTTON KEARNEY



Pressure without price

What record reported ransomware volumes, the shift to data theft, and a fourth year of falling premiums mean for boards and what to do while the window is open.

Contents

01

The paradox at a glance

Cyber insurance has rarely been more affordable.

Cyber risk has rarely been more consequential. Two statements are both true right now, at the same time, and reconciling them is the single most important thing a board can do with this report.

In the first half of 2026, recorded ransomware activity hit a fresh half year record. Data theft became a routine feature of almost every serious attack. Regulators sharpened their focus from whether an organisation was breached to what the breach revealed about its governance.

And yet cyber insurance pricing fell for a fourth consecutive year, with capacity abundant and carriers competing hard on both price and breadth of cover.

At first glance those trends look contradictory. They are not.

Attacks are becoming more frequent and their consequences more severe, while the insurance market is being held soft by a structural oversupply of capacity rather than by any easing of the underlying threat. The cost of transferring cyber risk has fallen, even as the cost of retaining it keeps rising.

The one line that reconciles everything

The market is not oversupplied for the risks that exist. It is over-supplied for the risks it has learned to price, and chronically under supplied for the ones it has not, autonomous AI-enabled attacks, systemic single vendor concentration, and long-tail data-theft liability among them. That gap between what can be priced and what is actually happening is the thread running through every page that follows.

What the half looked like, in four numbers

4,295
recorded ransomware events - a record half

60%
of all of 2025's volume, reached in six months

67%
of AU incidents involved data exfiltration (Q1)

4th
consecutive year of falling cyber premiums

Sources: RansomGraph (H1 2026); Wotton Kearney incident-response data (Q1 2026); Howden Re, Cygenesis (May 2026). Recorded / reported figures - see Section 02.

This report is a collaboration between three teams who each see a different face of the same problem. NSB Cyber brings the threat data - who is attacking, whom, and how. Wotton Kearney brings the legal and regulatory front line - what a breach actually triggers once the systems are back up. And Howden brings the market and boardroom view - what all of this means for how you finance, govern and transfer the risk.

Read together, there's only one story: the threat has outrun the data, and the window to act on favourable terms will not stay open forever.

02

How to read these numbers

Before the data, one essential caveat, because it changes how every figure in this report should be read.

The event counts here are recorded and reported events, not the true total.

Ransomware activity is counted primarily from what surfaces publicly: victims named on leak sites, incidents disclosed to regulators, and matters that reach specialist responders. That methodology, by design, misses a very large volume of activity. It does not capture organisations that paid quietly and were never posted, incidents settled before a leak deadline, attacks that were contained and never disclosed, or the vast number of events in jurisdictions and sectors with no mandatory reporting at all. Every credible source treats these counts as a conservative floor.

So throughout this report, where we cite figures such as "4,295 events" or "754 in manufacturing," read them as recorded events - a reliable measure of direction, scale and relative concentration, and a floor on absolute volume. The trend lines are real. The true totals are higher. That distinction is not a disclaimer to be skimmed; it is itself one of the most important findings in this report, because it means the exposure your organisation faces is larger than any public number suggests.

Why we know the real number is materially higher

The clearest evidence is in our own data and combined industry data. Leak site tracking only records victims whose stolen data was published online, but that misses most cases. Attackers publish data to pressure victims into paying, so those who do pay are often kept off the leak sites entirely, and many never report the incident at all. Between the victims who pay quietly and the many more who never pay but are never named, the population of organisations actually attacked is far larger than any leak site dataset shows. The recorded figure of 4,295 is best read as **the visible tip of a materially larger problem.**

03

The threat in the data

H1 2026 ransomware - a record half, and a leaderboard in motion.

Intelligence: NSB Cyber RansomGraph dataset - recorded events, 1 Jan - 30 Jun 2026

H1 2026 recorded 4,295 ransomware events (2,221 in Q1, 2,074 in Q2) - the highest six-month total on record, above both H2 2025's 3,619 and H1 2025's 3,560. The first six months of 2026 already represent roughly 60% of the entire 2025 total of 7,179. Global volume has now held above 2,000 recorded events for three consecutive quarters: a sustained plateau, not a short-term surge.

For context, a single quarter of 2026 now approaches three-quarters of what the entire year of 2021 recorded.

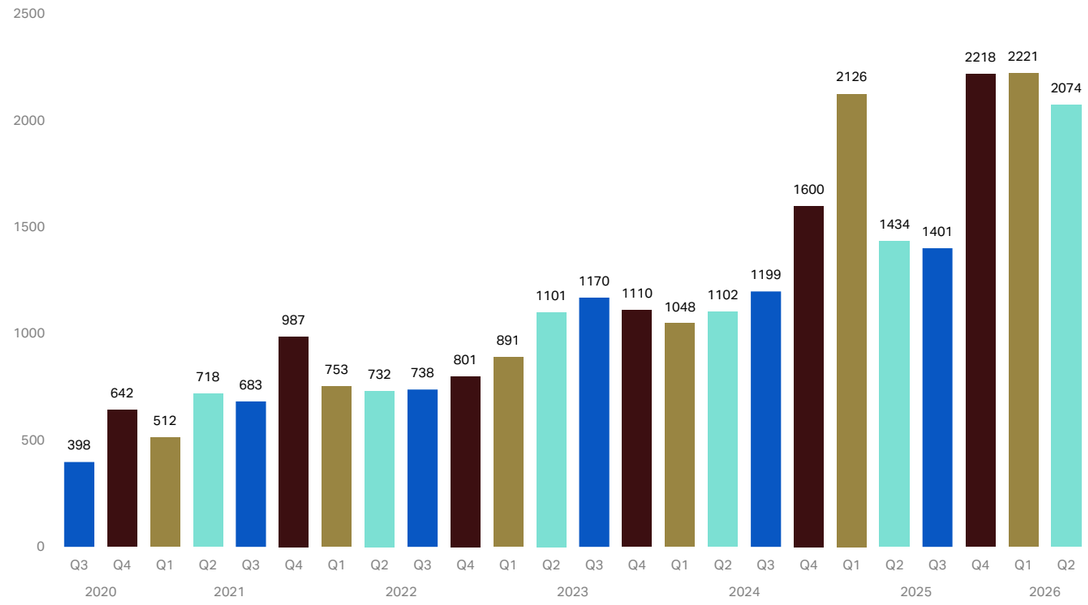


Figure 2: Top threat actors, H1 2026 (recorded events). Source: RansomGraph.

Fragmentation, not consolidation

The defining feature of the half is breadth, not concentration. A record 55 new actor brands emerged (27 in Q1, 28 in Q2) among 126 distinct active operators - the most of any half in the dataset. When a brand is disrupted, its affiliates and access demand do not disappear; they redistribute across competing programmes. RansomHub illustrates the mechanism: dark for a fifth consecutive quarter after its April 2025 collapse, with its affiliates largely absorbed by DragonForce, which has formalised a "cartel" model letting affiliates spin up their own brands on shared tooling.

Qilin remained the single most prolific operator with 664 events, but was the only top-tier group to contract - down 7.6% half on half and falling within the period from 384 events in Q1 to 280 in Q2, its lowest quarter since early 2025. Moving hard in the opposite direction, THE GENTLEMEN rocketed from a standing start to second place with 457 events - up 493.5% and still accelerating at half-end (200 in Q1 to 257 in Q2), the fastest sustained climb of any operator on record. Akira held third (278) despite a 22% decline; DragonForce rose 79% to 240; and LockBit rebounded 86% to 199 on the back of its 5.0 relaunch.

Where the attacks landed

Manufacturing & Industrial Products led all sectors with 754 events (up 18.9%), followed by Professional Services (596) and Engineering & Construction (467, up 32.3%). Together the top three accounted for roughly 42% of recorded activity; a meaningful plurality, but far from a monopoly.

The sharpest movers were structural rather than cyclical: Government & Public Sector rose 52%, and Legal Services entered the top table outright at 148 from a negligible base, as operators increasingly monetise privileged and confidential document stores. Healthcare & Life Sciences (322, up 20.6%) remained heavily exposed given the sensitivity of the data it holds.

Top sectors under attack

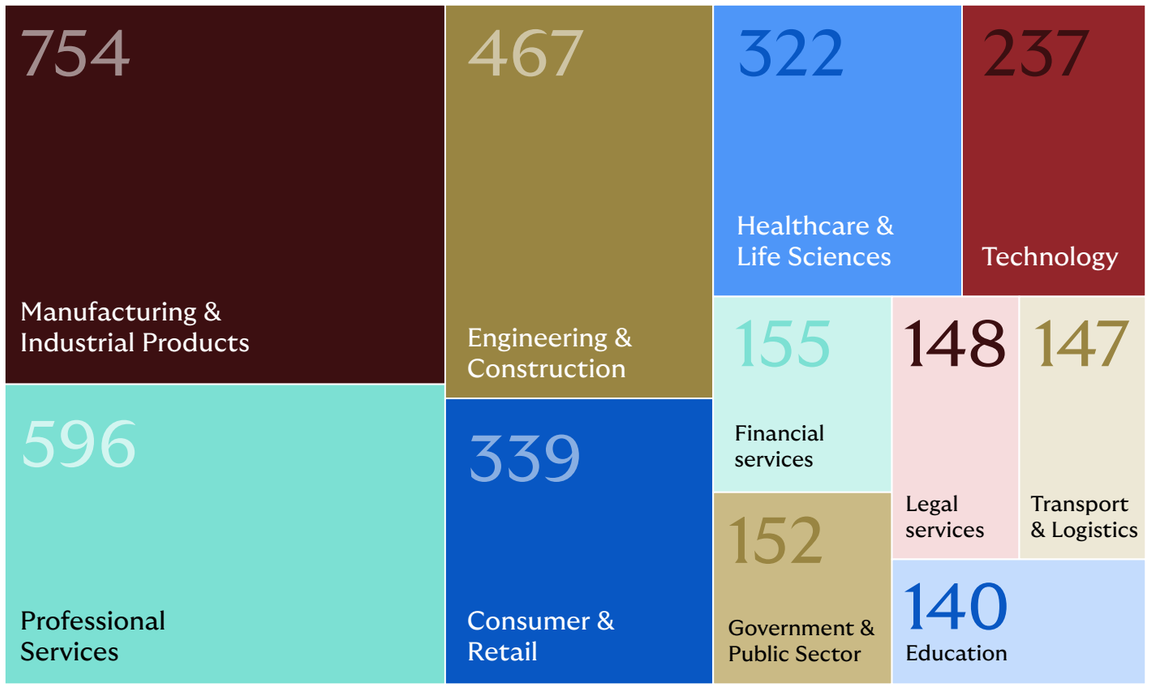
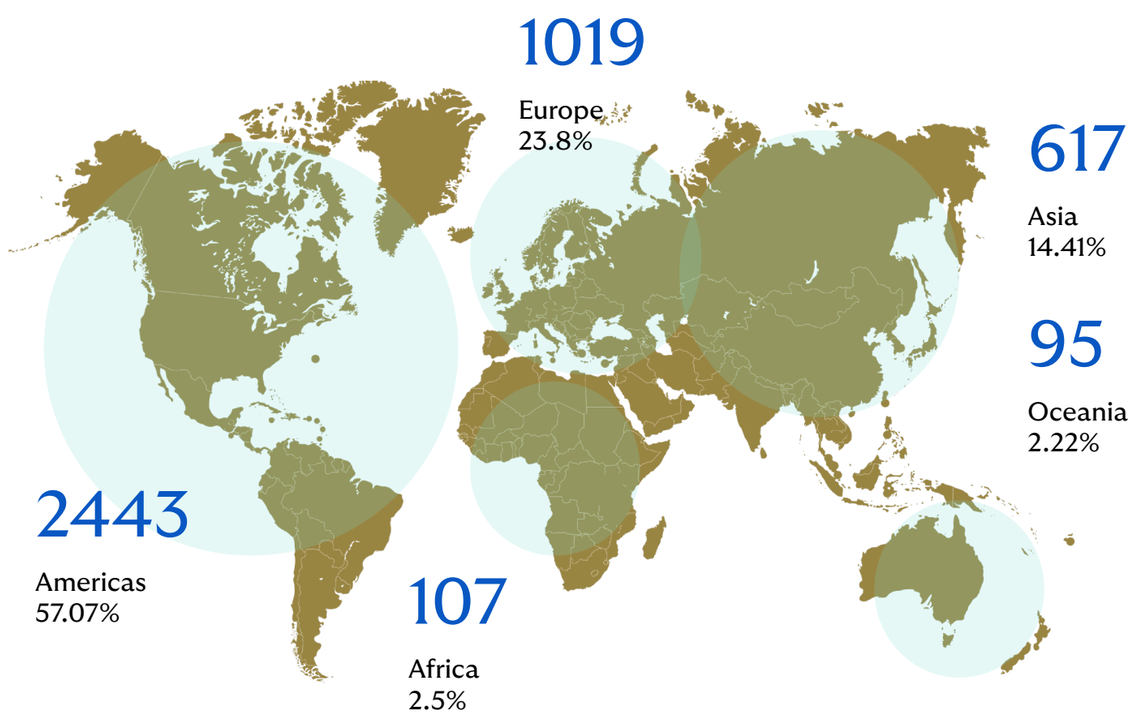


Figure 3: Top sectors under attack, H1 2026 (recorded events). Source: RansomGraph.

A record half for Asia & Oceania

The Americas remained the primary geographic centre at 2,443 events (57%), ahead of Europe (1,019) and Asia (617). But the standout regional story is closer to home: Asia and Oceania together set a combined record of 712 events, with each region logging 356 in Q1 and again in Q2 - well above the previous quarterly high of 317 and more than triple the 114 recorded in Q1 2024. Within Oceania's 95 events, Australia absorbed the overwhelming majority at 78, followed by New Zealand at 11. That concentration underscores Australia's exposure as the region's primary target - at precisely the moment its mandatory ransomware payment reporting regime moved onto an enforcement footing.



Asia & Oceania recorded events by quarter

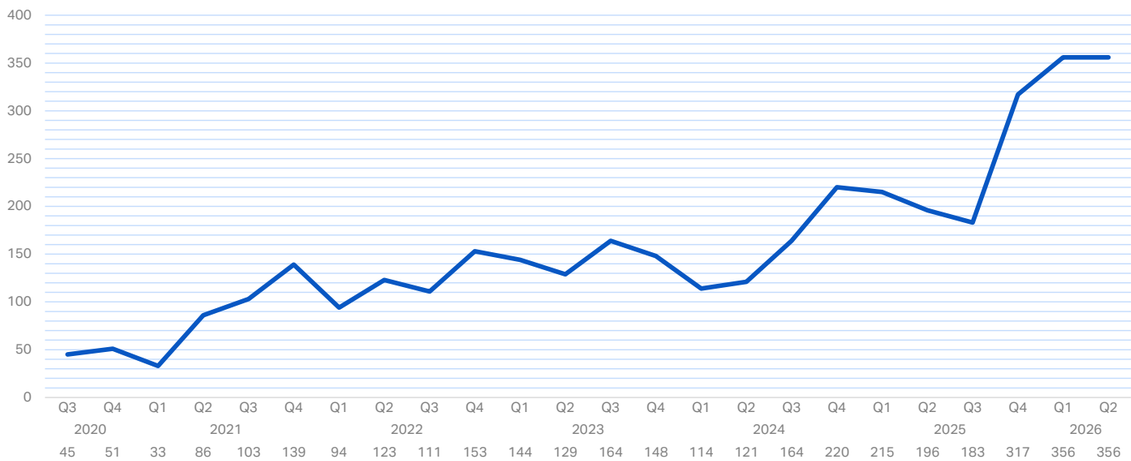


Figure 4: Regional distribution, H1 2026 (left); Asia & Oceania recorded events by quarter (right). Source: RansomGraph.

How they got in & the tradecraft that matters

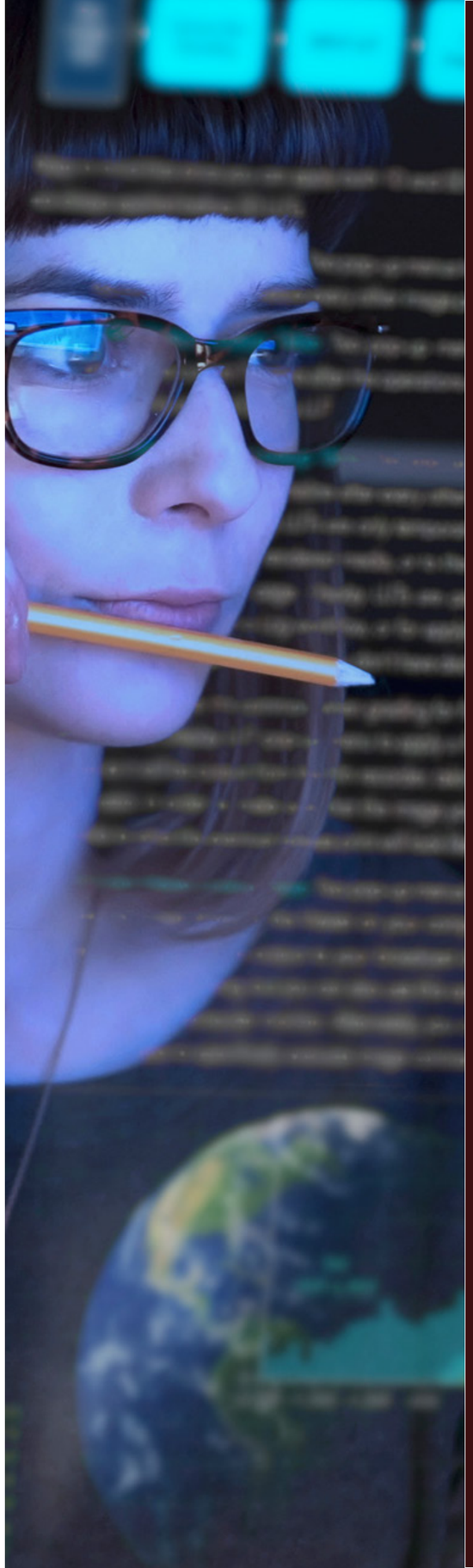
Across the leading operators, the front of the kill chain now converges on two entry points: exploitation of public-facing applications and abuse of valid accounts. The most significant shift in 2026 telemetry is that exploitation of internet-facing and edge devices has, for the first time on record, overtaken stolen credentials as the single most common initial-access vector - with edge-device and VPN exploitation rising roughly seven-fold as a share of exploitation-driven breaches. That keeps Fortinet, Ivanti, Citrix, Palo Alto, SonicWall, managed-file-transfer platforms and remote-access tooling as high-value targets wherever patch cadence lags.

Beyond the shared entry points, tradecraft diverges. Akira runs the broadest hands-on intrusion - SonicWall SSL-VPN exploitation (CVE-2024-40766), credential replay defeating MFA, BloodHound discovery and RClone exfiltration - frequently encrypting in under four hours. Clop is the specialist, centred on managed-file-transfer and ERP platforms (Oracle E-Business Suite, GoAnywhere MFT) in a data-theft-led model that often omits encryption entirely. The operational takeaway is sharper than before: as brands fragment, tracking recurring techniques across groups yields more durable defensive value than tracking actor names.

Evan Vougdis: A responder's outlook

Ransomware has moved from episodic surges to a sustained high-tempo baseline, and the ecosystem is now fragmented but resilient - no longer dependent on any single dominant brand. Expect sector pressure to stay concentrated where downtime, data sensitivity and third-party dependency create the strongest extortion leverage: manufacturing, professional and legal services, healthcare and technology providers. Perimeter-facing and identity-led intrusion will remain the primary drivers, with the help-desk-manipulation and MFA-reset playbook popularised by Scattered Spider still being replicated across the ecosystem.

The largest single escalation risk remains another repeatable exploitation pathway against a widely deployed SaaS, managed-file-transfer, edge-appliance or remote-access technology - a chain reaction that could reshape exposure inside a single quarter.



04

The shift that matters

From encryption to data theft & why the loss has quietly changed shape.

If there is a single trend that connects the threat data, the legal reality and the insurance market, it is this: **the centre of gravity in a ransomware attack has moved from encryption to data theft.**

Historically, ransomware losses were driven by encryption and operational disruption; systems locked, production halted, a ransom demanded to restore access. That threat has not gone away, but it is no longer the main event. Today, data exfiltration increasingly sits at the centre of the incident. Attackers steal first and encrypt second, if at all. A growing share of operators, the encryption-optional brands such as Coinbase Cartel, and specialists like Clop, skip encryption entirely and extort purely on the threat of publication.

This matters enormously for how a loss develops, and it is where our three datasets converge. NSB's threat data shows operators deliberately targeting data-rich, downtime-sensitive environments and moving into legal and government verticals that hold privileged documents. Wotton Kearney's incident-response data shows exfiltration in 67% of Q1 2026 matters. And Howden's market analysis shows why this should worry every buyer: data-driven losses behave completely differently from encryption losses.

The critical difference for a board

Encryption is visible immediately. The systems are down, the cost crystallises fast, and recovery is measurable. **Data-related liabilities are the opposite.** They emerge months or even years later, through regulatory investigations, customer complaints, contractual disputes, shareholder scrutiny and litigation. The same incident now costs more to handle even where no ransom is paid, and the most consequential part of the bill may not arrive until long after the incident is "over."

That long-fuse quality is the bridge to the two sections that follow. It is why the legal and regulatory consequences of a breach have become the real exposure (Section 05), and it is why the insurance market can keep softening even as risk rises - because the losses most likely to turn the cycle are precisely the ones slowest to surface (Section 06).

05

The consequence layer

Payments, privacy and the legal front line

Legal analysis: Wotton Kearney

Incident-response and regulatory practice: Australia, New Zealand & Asia

Most organisations are choosing not to pay

While ransom payments attract most of the headlines, the reality on the ground in Australia is that most organisations are choosing not to pay. In Wotton Kearney's experience, only 4% of cases over the past two and a half years involved a ransom payment - down from around 15% in 2023, as organisations get better at preparing for and responding to incidents. The Australian Signals Directorate reported 94 ransom-payment reports under the mandatory regime over a seven-month period, though some of those are not true ransom payments but rather bounty hunter payments, suspicious transaction reports, or multiple reports of a single incident.

Several factors are driving payments down. Paying a ransom is not a mitigating factor in Australia: APP entities, state and regulated organisations must still meet their legal, regulatory and notification obligations irrespective of payment. Specialist negotiators report that paying does not reliably prevent data being sold or published anyway, making "data-suppression" payments an unattractive proposition. The focus has shifted decisively toward preparation: containing the incident with the right specialist vendors, recovering from safe and reliable backups, and having business continuity plans that keep the organisation running until normal operations resume.

Data exfiltration is now the rule, and its consequences are severe

This is where the threat data and the legal reality meet. Wotton Kearney's data indicates that in Q1 2026, 67% of incidents involved data exfiltration, with a further 19% showing inconclusive evidence; meaning exfiltration is now present in the vast majority of cyber-attacks. Increasingly sophisticated AI tooling lets threat actors quickly identify and extract specific, high-value data assets in a short space of time, so organisations are discovering after the fact that commercially sensitive or harmful personal information, for both staff and customers, has been taken.

The result is that notification and privacy obligations are being triggered in more incidents than ever. Organisations must understand the impacted data quickly and issue notifications in compliance with their legal obligations. Regulators; the OAIC, APRA and ASIC among them, increasingly require specific information about the type, volume and age of the data impacted, and what safeguards applied. Most organisations struggle here: large, poorly mapped datasets, delays in identifying affected individuals, gaps in logging and evidence preservation, and the sheer prevalence of old data lingering on systems. The consequences are regulatory action, severe penalties, and lasting loss of trust.

There is a commercial dimension too, often overlooked. Contractual obligations embedded in commercial transactions frequently require disclosure of a cyber incident within very short periods, and sometimes grant counterparties extensive powers to demand information, or leave the affected organisation liable for compensation post-incident. Understanding privacy and contractual risk well before an incident occurs dramatically reduces the exposure an organisation faces afterwards.

ASIC's open letter: AI has compressed the timeline

In May 2026, ASIC issued an open letter which should read as a clear warning: the threat landscape has fundamentally shifted, and AI is compressing attack timelines to the point where traditional response cadences are no longer adequate. Activity from AI-enabled adversaries has surged by 89%, while breakout times have fallen roughly 70% between 2021 and 2025 to an average of just 29 minutes, with the fastest observed lateral movement occurring in 27 seconds.

ASIC's reference to FIIG Securities signals that a precedent is set: the regulator is prepared to act where cyber-related governance failures leave customers exposed to foreseeable harm. Crucially, ASIC is not introducing new obligations. It is demanding that existing frameworks are not merely designed but demonstrably executed. Boards and senior executives are on notice that oversight must operate at the speed compressed attack windows now require, a plan is not enough; resilience must be tested, embedded and capable of performing at speed. As response windows narrow, outcomes are increasingly determined before an incident is even detected, which makes the quality of pre-existing controls and governance decisive.

Wotton Kearney: the practical takeaway

The battle is now won or lost before the incident. With payments falling, exfiltration near-universal, and regulators focused on demonstrable governance, the organisations that fare best are those that have mapped their data, privacy and contractual obligations in advance, and that engage specialist legal advice the moment an incident occurs, so they can meet their obligations to clients, staff, customers and regulators inside the compressed timeframes those obligations now demand.

06

The market and the boardroom

Pressure without price: a soft market belies a hardening threat

Market analysis: Jack Bassett
Howden - Cyber & Technology Regional Leader, Pacific

Everything in the preceding sections; record volumes, near-universal data theft, AI-compressed timelines, sharper regulatory teeth describes a threat environment that is getting harder. And yet the cyber insurance market enters the second half of 2026 in its fourth consecutive year of rate softening. Understanding why is essential to using this market well.

Capacity without the demand to absorb it

Howden Re's May 2026 analysis, Cygenesis, confirms the softening and raises the obvious question of how much further pricing can fall before it finds a floor. The cause is not a fall in risk but a structural imbalance: capacity has expanded ahead of demand, leaving excess supply concentrated within a largely unchanged buyer base. The growth insurers planned for larger limits from big corporates, rapid international expansion, product simplification to unlock SME demand has not materialised to the extent expected.

Two patterns stand out. Rate deterioration has been sharpest in the larger revenue segments, where competition for high excess layers is most intense, while SMEs have proven more resilient to downward pressure. And renewal pricing has held up better than new business across all segments, reflecting a degree of portfolio stickiness for incumbents even as carriers compete aggressively for new accounts. International diversification, long seen as the next growth engine, has stalled too: the US share of the global market, once expected to fall toward 54% by 2030, is now projected to hold near 65%. For buyers this is a favourable backdrop; broader wordings and competitive premiums, particularly for well-run risks, but it rests on supply dynamics, not on any easing of the threat.

What could turn the cycle?

The instinctive assumption is that worsening loss experience will eventually force rates back up. That is directionally right, but the timing is far from certain. Drawing on analogues from property-catastrophe and D&O markets, Howden Re's analysis shows that market turns are rarely driven by any single factor, and that sustained unprofitability can persist for years before pricing responds, particularly where losses are slow to surface.

Two features make cyber unusually sensitive to a sudden turn. First, concentration: the top ten carriers account for roughly 40% of cyber premium, while reinsurance is even more concentrated, with the top ten holding around 87%. A strategic retreat by even one or two leading players could disproportionately affect available capacity and pricing. Second, limited diversification: cyber does not need a once-in-200-year catastrophe to harden. Howden Re's modelling suggests a loss comparable to a moderate property-catastrophe year, on the scale of 2008 rather than a tail event could be enough to dislocate the market given its structure.

Cutting the other way is the very shift described in Section 04. The market's last hardening (2019–2021) was driven by first-party ransomware claims that settled quickly, giving fast loss visibility and a sharp pricing response. Today's losses lean toward data breach and third-party liability, which develop over a much longer horizon. That delay between an event and full recognition of its cost means deterioration can stay hidden for longer, allowing softening to persist even as performance quietly weakens.

Accountability has moved firmly to the boardroom

Perhaps the most significant cyber development for 2026 is not technological, it is governance. Cyber risk can no longer credibly be characterised as an emerging issue or delegated solely to technology teams. For most organisations it now sits alongside financial, operational and regulatory risk as a board-level responsibility.

Regulators increasingly focus not on whether an organisation suffered an incident, but on what the incident reveals about governance, known vulnerabilities, third-party oversight, investment decisions, incident preparedness, escalation pathways and executive accountability. The practical test for directors is becoming straightforward: can the organisation demonstrate a defensible record of what risks were identified, what questions were asked, what actions were funded, what controls were tested and how oversight was exercised?

In this environment, governance becomes more than a compliance exercise. It becomes a risk transfer mechanism in its own right: strong governance improves resilience, supports insurability, strengthens regulatory outcomes, and reduces the likelihood that a cyber incident evolves into a management liability issue. The line between cyber risk and directors' liability risk is becoming increasingly difficult to draw.

Jack Bassett, Howden: The Window

"Cyber insurance has rarely been more affordable, yet cyber risk has rarely been more consequential. That disconnect won't exist forever. The organisations that gain the greatest advantage from today's market will be those that use this window to strengthen resilience, challenge assumptions, and prepare for a future where cyber incidents are not a question of if, but of how well the organisation is prepared to respond."

07

What this means for you

Actions while the window is open

The through line of this report is that today's conditions are a window, not a destination. Whether the market turns in twelve months or three years matters less than whether your organisation uses this period effectively.

The organisations that fare best will not be those that simply buy the cheapest policy, they will be those that use favourable conditions to strengthen resilience, secure appropriate limits, align their cyber, crime and management liability programmes, and build the governance framework that regulators, insurers and stakeholders now expect.

Below, the priorities split by role.

Who	What to do with this window
CEO	Treat cyber as a board-level enterprise risk, not an IT line item. Own the narrative that a strong governance record is now a risk-transfer asset in its own right. Sponsor a tested incident response and business continuity capability, regulators and insurers increasingly reward organisations that can show resilience is embedded and rehearsed, not merely documented.
CFO	Recognise the asymmetry: the cost of transferring cyber risk has fallen while the cost of retaining it is rising. Use the soft market to secure appropriate limits and broader wording now, before the cycle turns. Align cyber, crime and management liability towers so a single incident does not fall into a gap between them. Model the long tail data liability exposure that may not surface for years.
Risk Manager	Map the actual data and dependency graph before an incident, not during one, including single vendor and supply chain concentration. Confirm your programme responds to data theft and third-party liability, not just encryption and business interruption, with aligned conditions such as appropriate waiting periods and periods of indemnity. Pressure test where the loss would migrate to the least clear wording, and close those gaps while capacity is abundant and competitively priced.
CISO	Prioritise the vectors the data actually shows: internet facing and edge device exploitation (now the leading initial access vector), identity and help desk manipulation, and rapid data exfiltration. Assume breakout in minutes, not hours; ASIC cites an average of 29 minutes. Invest in detection and logging that will stand up to a regulator asking precisely what data was taken, when, and what safeguards applied.

Five cross-cutting priorities

- **Assume the true threat is larger than any published number.**
  Recorded events are a floor; plan for the volume that never surfaces.
- **Prepare for data theft, not just downtime.**
  The most consequential costs now arrive months or years after systems are restored.
- **Buy breadth while it is competitively priced.**
  Wording discipline beats price - the loss migrates to wherever cover is least clear.
- **Make governance demonstrable.**
  Regulators now judge the record of oversight, not merely whether an incident occurred.
- **Rehearse for compressed timelines.**
  With breakout measured in minutes, preexisting controls and legal readiness decide the outcome.

08

Final word

The first half of 2026 has sharpened, rather than resolved, the central tension of this market.

Recorded ransomware activity set a fresh half-year record; data theft became a routine feature of serious incidents; AI compressed attack timelines into minutes; and regulators moved decisively toward judging governance rather than misfortune. And yet capacity is abundant and rates keep falling. The most candid framing is the simplest: the issue is not the volume of capacity but its aim, the risks the market can price sit alongside a growing set it still cannot.

Three things follow.

1. The numbers you can see are a floor; the real exposure is larger and should be planned for as such.
2. The loss has changed shape: prepare for long-tail data-theft liability, not just the encryption event that makes the headlines.
3. This is a window: a market less than 1% the size of the risk it covers, softening into a threat that is hardening, rewards those who lead on insight, resilience and governance - not those who lead on discount.

The posture that fits the moment

The cyber market remains soft. The threat environment is not. Nor is the accountability that comes with it. The market is **soft, but not naive** – that remains the right posture.

09

Methodology, sources & contacts

A note on methodology

The ransomware event data in this report is drawn from the RansomGraph dataset (data pulled 11 July 2026), which records ransomware activity from publicly observable sources including leak-site postings. As set out in Section 02, these figures represent recorded and reported events and should be treated as a conservative floor on true activity: they exclude organisations that paid without being published, incidents resolved before disclosure, and events in jurisdictions or sectors without mandatory reporting. Incident-response statistics are drawn from Wotton Kearney's Australian practice (Q1 2026 and rolling multi-year data). Market analysis draws on Howden Re's Cygenesis (May 2026) and related Howden cyber market data. Figures are cited for direction, scale and relative concentration.

Selected sources

RansomGraph - H1 2026 ransomware dataset (recorded events, TLP CLEAR). Wotton Kearney - incident-response and regulatory practice data, Q1 2026. Australian Signals Directorate - mandatory ransom-payment reporting. ASIC - open letter on AI-accelerated cyber threats (May 2026). Howden Re - Cygenesis (May 2026). Howden - 2025/2026 cyber market reporting. 2026 industry telemetry on initial-access vectors and edge-device exploitation. CrowdStrike - Global Threat Report (2026).

Contact the team

This report is a collaboration between Howden, Wotton Kearney and NSB Cyber. To discuss what it means for your organisation, your threat exposure, your legal and regulatory readiness, or your insurance programme. Please contact your Howden representative or the relevant partner team.

Howden

Market, coverage & placement

E cyberandtechnologyANZ@howdengroup.com

Jack Bassett

Cyber & Technology, Pacific

E jack.bassett@howdengroup.com

Aloisé Robinson

Cyber & Technology

E aloise.robinson@howdengroup.com

NSB Cyber

Threat intelligence & data

Brittany Buswell

E brittany.buswell@nsbcyber.com

Evan Vougdis

E evan.vougdis@nsbcyber.com

Wotton Kearney

Legal, privacy & regulatory

Nicole Gabryk

E nicole.gabryk@wottonkearney.com

Kieran Doyle

E kieran.doyle@wottonkearney.com

HOWDEN

www.howdeninsurance.com.au