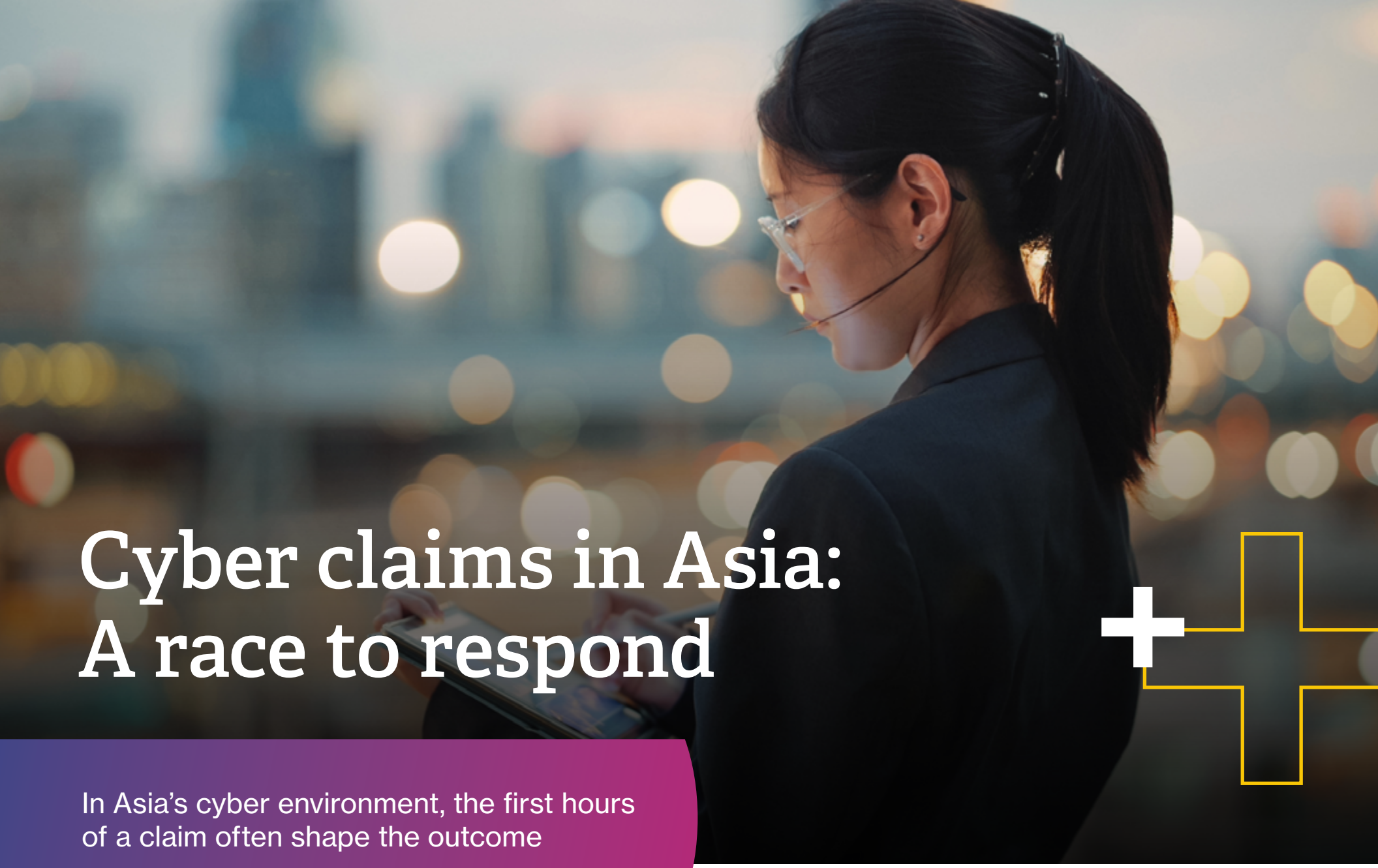


# Cyber claims in Asia: A race to respond

In Asia's cyber environment, the first hours of a claim often shape the outcome

Crawford®

Global Technical Services

$3.67M

AVERAGE DATA BREACH COST IN ASIA IN 2025.

*IBM, 2025*

78%

OF ORGANISATIONS IN ASIA PACIFIC REPORTED EXPERIENCING AT LEAST ONE CYBER INCIDENT IN THE PAST 12 MONTHS

*CLOUDFLARE, 2023 SURVEY*

# Cyber claims in Asia at a glance

## Cyber risk is now part of day-to-day business in Asia. Recent data shows that cyber incidents in Asia rose by 29% year on year, with the region accounting for over a third of global attacks.

From large corporates to SMEs, organisations across Asia are increasingly exposed to ransomware, social engineering, and data breaches as digitalisation accelerates. Yet cyber insurance uptake remains low, particularly among SMEs, where fewer than 10% are estimated to carry dedicated cyber cover. While larger organisations often have greater resources and more mature cybersecurity programmes, SMEs are typically less equipped to manage a major loss, widening the gap between exposure and protection.

The financial impact can be substantial. The average cost of a data breach in Asia is estimated at US$3.67 million, based on an IBM study of 600 organisations and excluding very small and very large breaches. The analysis highlights the cost of disruption, business interruption, regulatory scrutiny, and reputational damage that can follow a serious cyber incident.

The claims landscape is driven by both frequency and severity. Business email compromise, funds transfer fraud, and social engineering remain among the most common causes of cyber claims, particularly in Asia's trade-driven economies. At the same time, ransomware remains the largest driver of loss, accounting for an estimated 50–60% of large cyber claims by value. Increasingly, these attacks involve data theft and extortion, with data exfiltration present in around 40% of major losses, adding further regulatory and reputational exposure.

Once operations are disrupted, business interruption becomes the primary cost driver, often outweighing the initial trigger and turning a cyber incident into a broader operational and financial crisis.

# A market that moves fast

Cyber claims move quickly because the facts move quickly. Logs get overwritten, and systems are restored before critical evidence is preserved. Payment instructions are acted on before the fraud path is clear. Privacy timelines begin running from discovery, not from first notice to the insurer.

Many organisations operate across borders, with shared vendors and complex supply chains. A single incident can affect several business functions, locations, or service providers at once, drawing in multiple stakeholders and creating competing priorities.

That is why early coordination is critical: establishing the facts, keeping the response focused, engaging the right specialists, and maintaining a clear view of how the loss is developing. When structure is introduced early, evidence is more likely to be preserved, recovery efforts remain aligned, and business interruption can be contained.

# The claims driving the market

The current claims landscape in Asia focuses on three themes: ransomware, social engineering, and data exfiltration. Ransomware remains the leading cause of loss, while social engineering and business email compromise are the fastest-growing categories driving a large share of both claim count and claim spend. Supply chain and third-party incidents are also rising, reflecting Asia's deep integration with global IT and vendor networks.

A file may start with a mailbox compromise, a weak remote access point, or a vendor issue, then turn into an interruption problem, a privacy review, and a coverage discussion within days. Once that happens, the cost curve usually moves quickly.

> "Cyber claims develop incredibly fast, and the early response has to match that pace to contain loss, preserve evidence, and protect recovery opportunities. Decisive action at the outset is what keeps the loss controlled rather than compounded."
>
> Brendan Leon, cyber specialist

> In cyber claims, the risk of malware propagation is high. What drives the outcome is a prompt and coordinated incident response that contains the threat and accelerates recovery."
>
> Satoshi Yamazaki, Head of Cyber & Marine

# Business email compromise and social engineering

Business email compromise and social engineering are among the most common cyber losses affecting Asian businesses. The pattern is familiar. An attacker gets into an email account or convincingly imitates one, inserts a payment request into a real conversation, and leans on urgency and familiarity to get the money moving.

What has changed is the reliability of the signals people use to decide whether something is real. Voice, video, caller ID, and writing style all carry less weight than they once did. Deepfakes and AI-enabled impersonation have pushed that even further. Help desks and service desks have become attractive targets because they sit close to identity, passwords, and device enrolment.

That changes what matters in the first hours of a claim. The priority is to establish the scope of the compromise and coordinate the response. Early triage helps identify what happened, who was affected, what controls were bypassed, and whether the incident extends beyond a single transaction. Keeping the various stakeholders aligned – from the insured and insurer to banks, forensic specialists, and IT teams – can be critical to containing loss and preventing a fraud event from developing into a broader cyber claim.

Funds recovery opportunities can be time-sensitive, affected accounts may need to be secured, and evidence needs to be preserved before it is overwritten or lost. The earlier the facts are established and the response coordinated, the greater the opportunity to preserve recovery options and limit the overall impact of the loss.

# Ransomware

Ransomware remains the most disruptive cyber loss for many insureds because it puts pressure on operations, legal review, communications, and leadership all at once.

In Asian claims data, ransomware remains the leading cause of loss, accounting for around 50–60% of large claims. The model has also changed. Encryption is still common, though more events now include data theft, extortion, or threats of public disclosure. That shift changes what drives severity. In many files, the biggest issue is not the ransom demand. It is the interruption period, the scope of data review, the customer fallout, and the time it takes to restore operations.

The route in is rarely surprising. Weak remote access controls, poor identity hygiene, vulnerable public-facing systems, and help desk manipulation continue to appear in serious files. Once inside, threat actors move quickly. They disable tools, expand access, and go straight to the systems that will create the most pressure.

Shared platforms raise the stakes. A vendor or managed service provider compromise can create the same operational consequences as a direct attack on the insured's own environment while affecting several policyholders at once.

Recovery readiness is often what separates a manageable cyber incident from a costly business crisis. Across Asia, local subsidiaries may face resource constraints, limited cybersecurity expertise, or uneven adoption of group-wide security policies. As a result, vulnerabilities can remain unresolved and critical response actions delayed, increasing both operational disruption and financial losses.

# Why these files get complicated quickly

Asia's regulatory landscape is complex, with privacy obligations spanning multiple countries. Many insureds depend on regional or global vendors, complicating evidence handling and legal coordination. The diversity of languages, legal frameworks, and business practices across the region frequently necessitates local expertise to support effective investigation and recovery.

Third-party concentration now plays a bigger role in claims severity. Many organisations rely on a small number of core providers for cloud infrastructure, communications, payments, and managed IT. When one of those providers fails or is compromised, the problem reaches farther and lasts longer.

Data governance also matters more than many insureds realise. Excessive retention widens the review, prolongs legal work, and increases response spending. Poor data discipline changes the economics of the file.

Late notice remains a recurring challenge. Some insureds start remediation before anyone has preserved logs, isolated the right systems, or determined who did what. That makes the technical story harder to reconstruct and narrows the path for recovery later.

> For every insurer writing cyber risk in Asia, the speed and quality of the claims response is critical to loss mitigation."

Satoshi Yamazaki, Head of Cyber & Marine

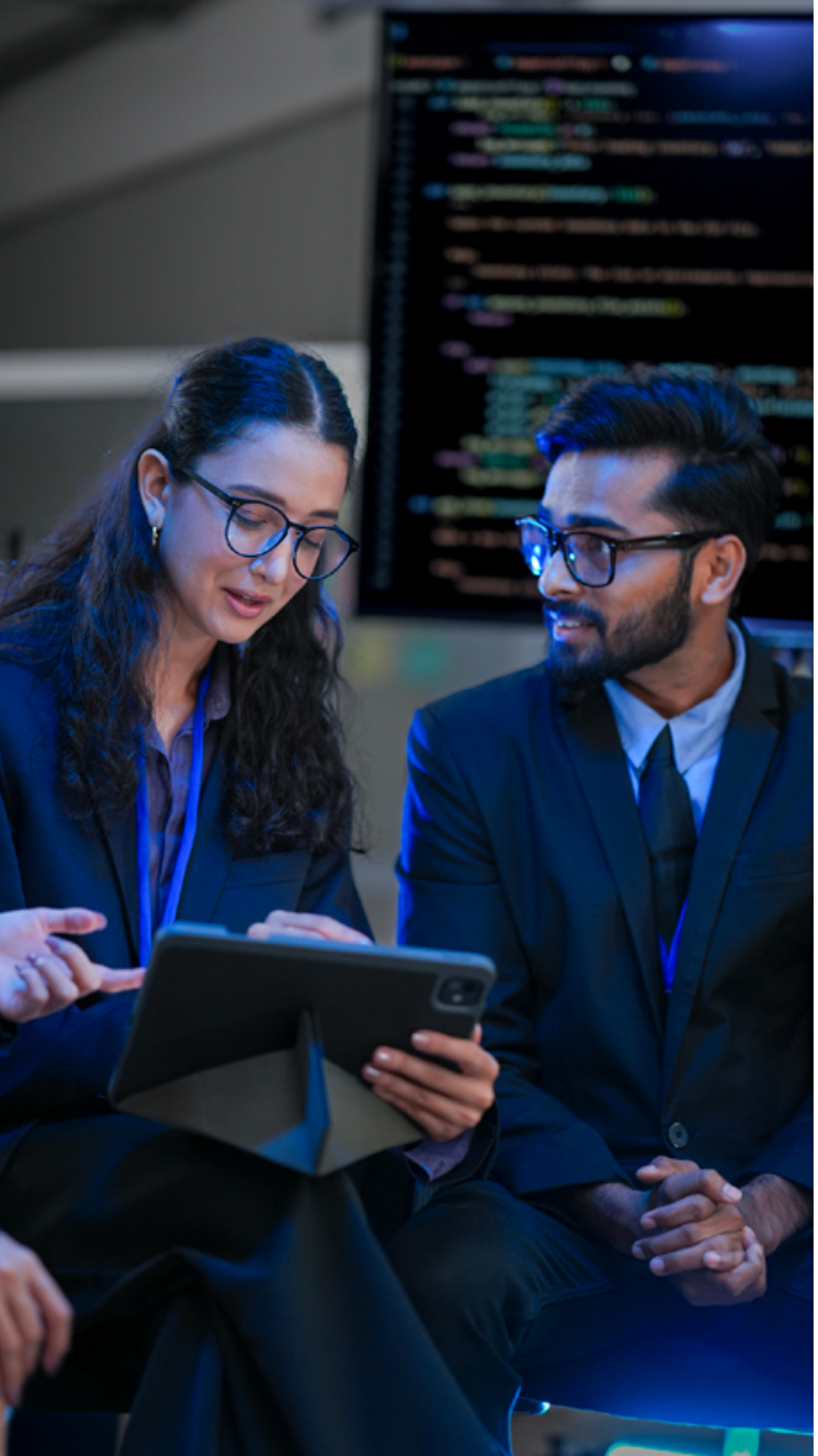
# Where severity builds

In many cyber incidents, the greatest cost is not the technical breach itself but the disruption that follows. When operations are interrupted, losses accumulate rapidly – revenue is impacted, staff are diverted from core activities, customers and suppliers are affected, and leadership must focus on crisis management rather than running the business. The longer the interruption persists, the greater the financial and reputational consequences.

Contingent business interruption now matters as much as direct interruption in many files. A cloud provider outage, SaaS failure, payment processor incident, or managed service provider compromise can produce the same commercial damage as a direct attack on the insured's own systems.

That is why BI and contingent BI function as claim multipliers. They expand what might have been a contained technical incident into a broader operational loss.

The relationship between interruption and extortion is practical. The decision around a ransom often sits beside the question of how long the business can stay impaired. That decision depends on the quality of backups, the pace of restoration, the credibility of the threat actor, and how quickly the response lines up with the commercial reality of the loss.



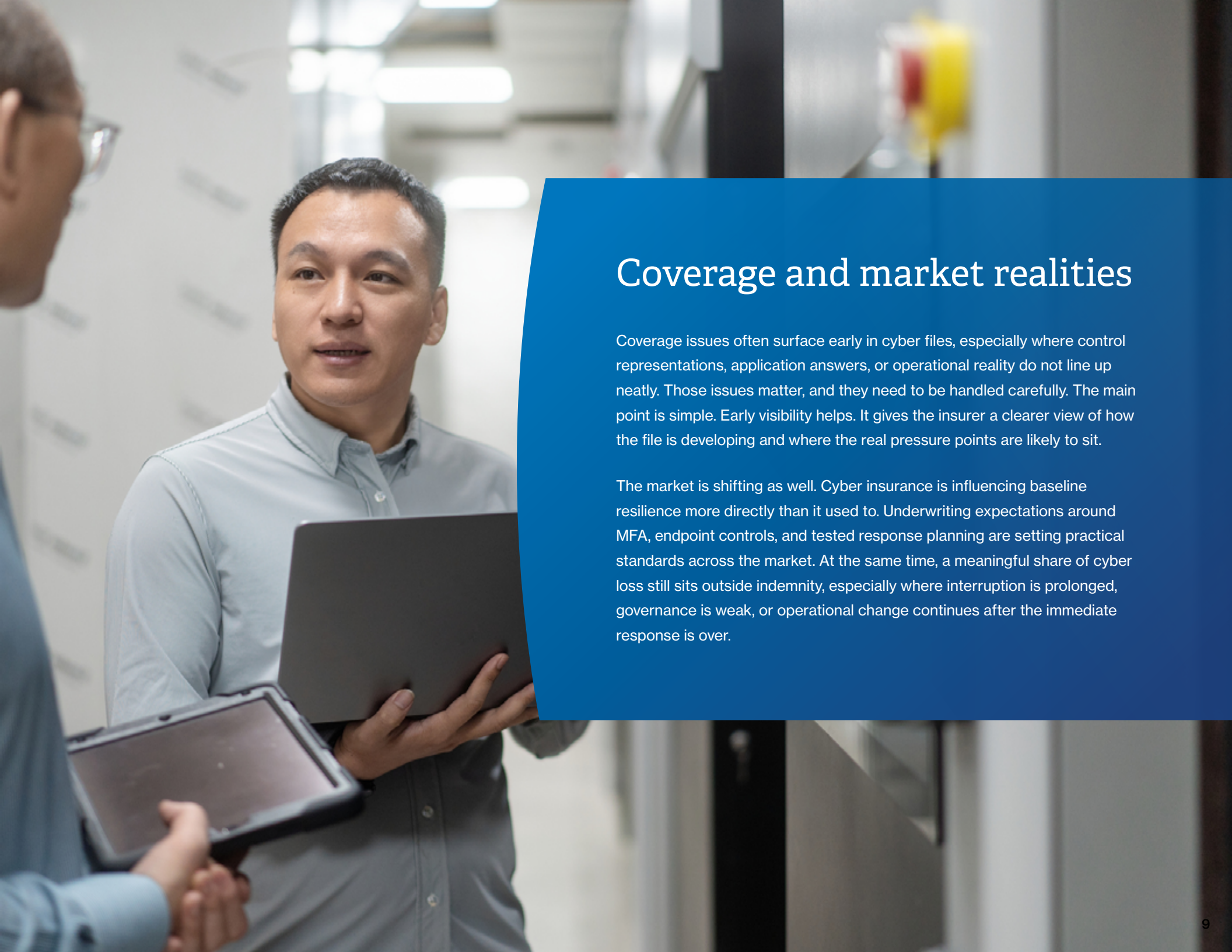
# What changes the outcome

Serious cyber claims attract a crowd quickly. Forensics experts, lawyers, communications advisers, internal IT, leadership, banks, and vendors may all become involved within hours. In a fast-moving environment, early coordination is critical.

Initial triage plays a central role. Understanding what happened, what systems or data may be affected, whether operations are disrupted, and what immediate actions are required helps shape the entire response.

Preparation plays a large role here. Pre-established response vendors, clear decision-making authority, alternative communication channels, and practical tabletop work matter. The strongest files usually come from organisations that had already worked through who decides what, how communications continue if core systems are unavailable, and which outside partners can actually respond when called.

The same is true for cost control. The first 24 to 48 hours influence the size of the notification review, the quality of the forensic findings, the pace of restoration, and whether recovery opportunities are preserved. Good files tend to have one thing in common: the process stays tight.



# Coverage and market realities

Coverage issues often surface early in cyber files, especially where control representations, application answers, or operational reality do not line up neatly. Those issues matter, and they need to be handled carefully. The main point is simple. Early visibility helps. It gives the insurer a clearer view of how the file is developing and where the real pressure points are likely to sit.

The market is shifting as well. Cyber insurance is influencing baseline resilience more directly than it used to. Underwriting expectations around MFA, endpoint controls, and tested response planning are setting practical standards across the market. At the same time, a meaningful share of cyber loss still sits outside indemnity, especially where interruption is prolonged, governance is weak, or operational change continues after the immediate response is over.

# Claim response study

► ADJUSTER ACTION ♦ DECISION POINT ⚑ COVERAGE CONCERN

| HOUR 0<br>DISCOVERY | HOURS 1-12<br>CONTAINMENT | DAYS 1-2<br>COMPILATION | DAYS 3-7<br>NEGOTIATION & RECOVERY | WEEK 2+<br>RESOLUTION |
|---|---|---|---|---|
| ► 6PM Friday - loss reported. Immediate triage. Systems down; potential data exposure identified. | ► DFIR and breach counsel engaged immediately. Privilege established on first call. | ► Backups encrypted and not isolated. Restoration not viable. Ransom negotiator engaged. | ♦ Ransom path confirmed with insurer and counsel. Sanctions reviewed; negotiations advance. | ► Forensic work concludes. Root cause confirmed. Operations restored. |
| ► Vendor response requirements defined on first call. | ► Hourly insurer updates begin. Policy reviewed for initial coverage position. | ⚑ Backup controls inconsistent with application. Potential misrepresentation identified. | ♦ Forensics vs restoration managed. Evidence preserved before system rebuild. | ⚑ Misrepresentation confirmed post-forensics. Coverage position finalized. |
| | ♦ Regulatory notification obligations and timelines assessed. | ♦ Critical path letter issued within 48 hours. Rights reserved as response continues. | ► BI impact assessed. Reserves updated as scope expands. | ► BI period quantified and closed. Subrogation potential assessed. |

# Closing

Cyber claims in Asia are getting more layered, more operational, and more dependent on what happens in the first days of the response. The files that go well usually have a few things in common. The facts are gathered early, the response stays organised, the right specialists are in place, and the commercial reality of the loss stays visible throughout.

That is where outcomes are shaped. It affects containment, downtime, evidence quality, reserve stability, recovery options, and the path to resolution. It also affects what happens after the file closes, including regulatory follow-through, recovery efforts, and the insured's ability to steady itself for the next event.

Cyber exposure will keep growing, and the claims will keep getting more layered. The files that are handled well will keep standing out for the same reason. The response stayed focused, the facts stayed clear, and the loss was managed before it had the chance to spread.

---

*The statistics cited in this report are drawn from third-party industry and government sources and reflect published estimates available at the time of writing. Figures may vary based on incident type, organization size, reporting methodology, and scope.*

For further discussion on cyber response strategies, visit our website.

# About Crawford & Company®

For over 80 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.

**10K** employees | **50K** field resources | **70** countries | **$18B** claims managed annually

Crawford® GTS

Learn more at
www.crawco.com

CRAW-BROCHURE-ASIA CYBER-0726