Marsh

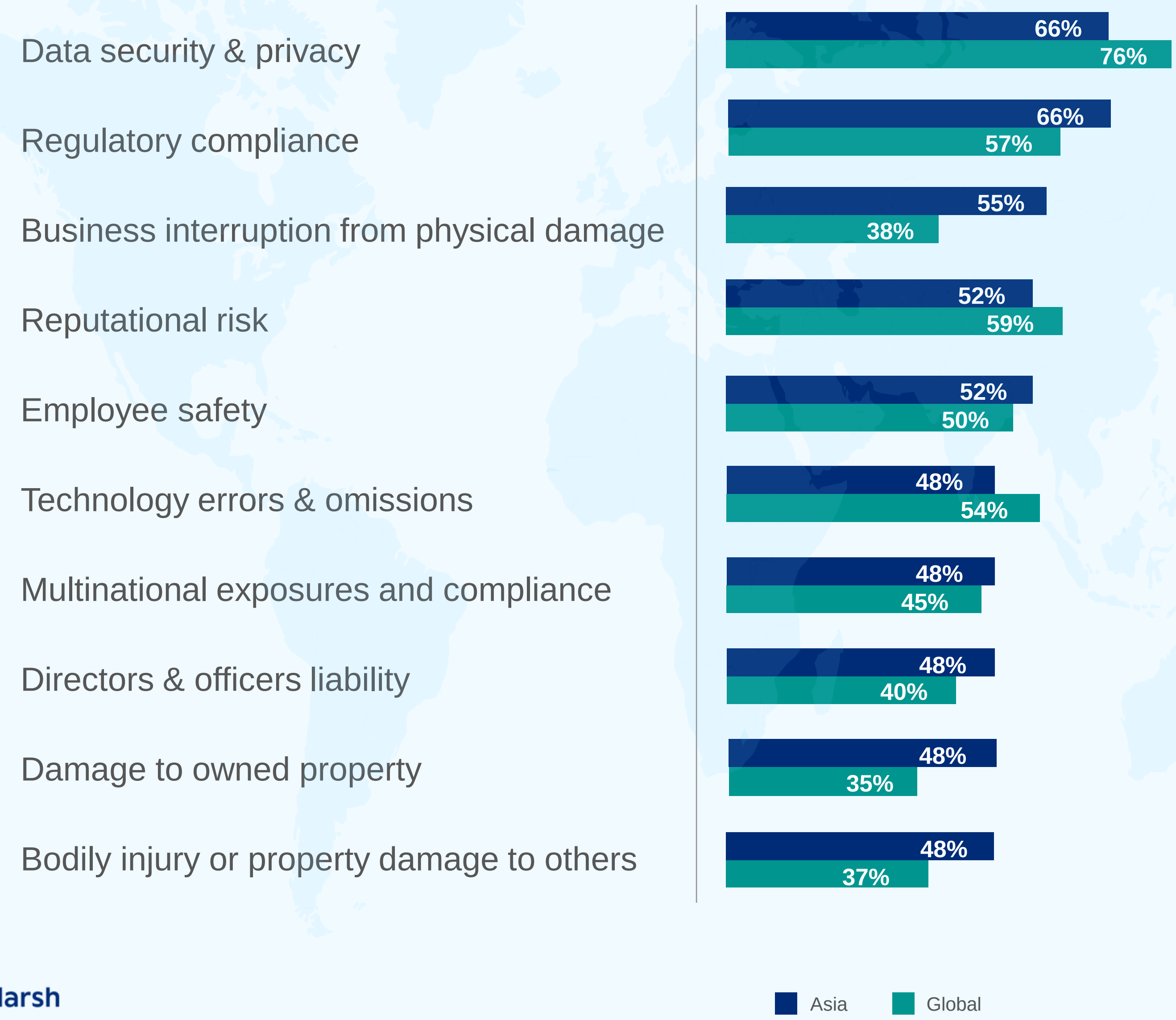
2024 Top 10 Risks in Asia's Technology Industry

Seizing opportunities despite rebounding risks

July 2024

A business of Marsh McLennan

Top 10 risks perceived by companies in Asia vs. Global in 2024



Key observations:

1

Data security & privacy surged to

#1 risk from #10 in 2023

2

Regulatory compliance moved 6 spots to

#2 risk from #8 in 2023

3

Business interruption from physical damage rose to

#3 risk from #14 in 2023

4

Employee safety moved to

#5 risk from #16 in 2023

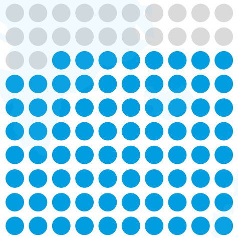
Marsh

The return of Asia's top tech risk

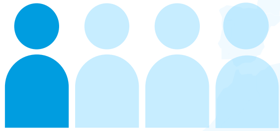
Data security & privacy

2024
1st

2023
10th



78%
indicated artificial intelligence (AI) as a risk concern.



Only 1 / 4
taking formal actions to understand current or potential AI risks.

This is exemplified by the surge in ransomware attacks in APAC, rising 39% year-on-year[1], and the increased risk of cyber/tech related crimes[2] due to rapid AI adoption.

According to [Marsh-Microsoft's report on The State of Cyber Resilience](),

69% of Asia's respondents are confident in their organisation's cyber risk management program.

35% evaluate the cyber risk of new technologies when a cyberattack or incident has occurred.

[1] Channelasia.tech (2024).Ransomware attacks in APAC on the rise
https://www.channelasia.tech/article/1310321/ransomware-attacks-in-apac-on-the-rise.html

[2] Channel News Asia (2024). AI in Southeast Asia: As new frontier opens in scams and cyberbullying, authorities wage high-tech battle
https://www.channelnewsasia.com/asia/artificial-intelligence-southeast-asia-deepfakes-cyberbullying-scams-cybersecurity-threats-4159006

Marsh

> **Asia's tech companies should chart a clear cyber resilience roadmap to identify, evaluate and act on the cyber risk scenarios that their businesses face.**

Christopher Lindsey
Strategy & Growth Leader,
Marsh Consulting, Marsh Asia

Larry Liu
Communications, Media and Technology (CMT)
Industry Leader, Marsh Asia

What should companies do to develop their roadmap to **Cyber Resilience:**

How is your organisation at risk?
- Cyber Exposure Quantification
- Cybersecurity Self-Assessment
- Operational Technology Cyber Health Check

What risk strategies are right for you?
- Enterprise Risk Management (Total Cost of Risk Optimisation)

How can you build cyber resilience?
- Cyber & Captive insurance placement
- Cyber Risk Consulting
- Cyber Incident Response (Crisis Management Simulation + Claims Advocacy)
- Post event review

Tech companies face increased scrutiny in physical and digital worlds

Regulatory Compliance

2023
8th

2024
2nd

Compliance in the digital world

Regulators are updating and proposing new rules for digital business models. This includes e-commerce compliance with anti-monopoly, information collection, IP, and commodity quality laws.

Examples
- E-commerce Law of PRC
- China's (PCRI) Law
- The UK Online Safety Bill (OSB)
- EU's Digital Service Act and Digital Markets Act

Compliance in the physical world

Geopolitical tension, trade wars, and climate change lead to export control, tax laws, tariffs, sanctions, and carbon emission regulations by markets such as the US and Europe, which impact Asia's manufacturers. Tech companies also face scrutiny from consumer protection laws.

Examples
- China's Law on the China's Protection of Consumer Rights and Interests (PCRI)
- US CHIPS and Science Act
- Clean Energy Requirement (Singapore)

What should companies do to ensure **compliance and to mitigate risks:**

Navigating complex regulatory frameworks and geopolitical tensions requires holistic and integrated risk management, which is crucial for businesses in the region to build trust, manage reputational risks, and ensure compliance with local customs and regulations.

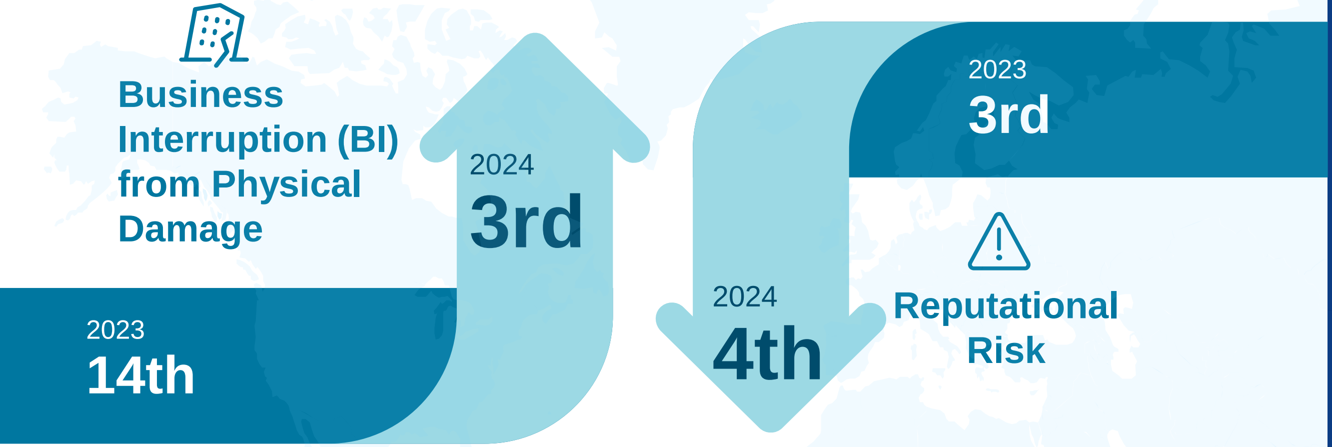
Build up business resilience with **Business Continuity Management (BCM)** measures

A clear plan to identify risks as part of your organisation's **Enterprise Risk Management (ERM)**

Enhance cyber risk resiliency through **advisory services** and **technologies for insurance**, **incident management**, **risk intelligence**, and **resilience optimisation**.

Have in place proper processes to fulfill **Task Force on Climate-Related Financial Disclosures (TCFD)**'s recommendations in terms of governance, strategy, risk management metrics and targets.

Physical damages also causes reputational losses



With Asia hit hardest by extreme weather[3], it is no surprise that tech companies in our region are more concerned about BI from physical damage compared to their global counterparts (55% vs 38%). In 2024, a 7.4 magnitude earthquake in Taiwan caused up to $1.0 billion in insurable losses[4].

However, consequential BI often exceeds direct physical damage in the tech sector. Events like power outages, fires, or natural disasters can result in reputational losses, contract losses, and declining client trust and market value.

[3] The Straits Times (2024). Asia hit hardest by climate, weather disasters in 2023: UN https://www.straitstimes.com/asia/asia-is-most-climate-disaster-impacted-region-un-meteorological-agency-says

[4] CoreLogic. (2024). Mw 7.4 Earthquake Rattles Eastern Taiwan https://www.corelogic.com/intelligence/blogs/hazard-hq/earthquake-rattles-eastern-taiwan/

Marsh

Take measures to answer pertinent questions on BI:

- How long would it take my business to recover from an event?
- What is the maximum foreseeable loss (MFL) exposure and Anticipated Maximum Business Interruption Loss (AMBIL)? Do my current internal processes and BI worksheet capture my risk exposure?
- Are there gaps in my current coverage? What adjustments should be considered?

What should companies do to enhance resiliency against **Business Interruption (BI):**

Risk Assessment

Identify and evaluate BI risks specific to businesses such as natural disasters, supply chain dependencies and other regional-specific risks

Risk Mitigation

Implement risk control measures, such as improving infrastructure resilience, diversify suppliers and reduce dependencies

Crisis Management and Response

Test crisis management plans annually and coordinate communication efforts to manage impact

Business Continuity Planning

4 step process: Impact analysis, recovery strategies, effective operationalisation and test, maintain & enhance processes

Insurance Solutions

Obtain appropriate insurance coverage including property damage and business interruption (PDBI), parametric, product recall coverage to protect against BI

Employee safety resurfaces as risk due to global supply chain diversification

Due to geopolitical tensions and trade wars, Asia tech companies need to relook their supply chain strategies to reduce dependencies on one location. As tech companies such as Foxconn and TSMC diversify their supply chains across Southeast Asia[5], they expose workers to different regulatory environments, safety standards, and risks.

What should companies do to address **employee safety and well-being**

Ensure physical safety: Implement safe work practices, fire and life safety audits, and workplace injury claims defensibility.
Explore better working conditions: Adhere to ESG standards, such as environmentally sustainable practices that reduce operational hazards.

Provide relevant benefits: Offer benefits that support employees' psychological and financial well-being such as free/subsidised food and housing.

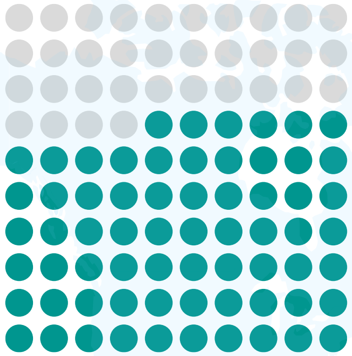
Obtain feedback: Conduct regular employee listening surveys to address safety concerns effectively and in a concerted manner.

Do you know?

According to Mercer's Global Talent Trends 2024, financial strain is one of the top reasons leading to burnout. Providing benefits related to finances including free/subsidised food or housing helps to create a safety net psychologically for employees.

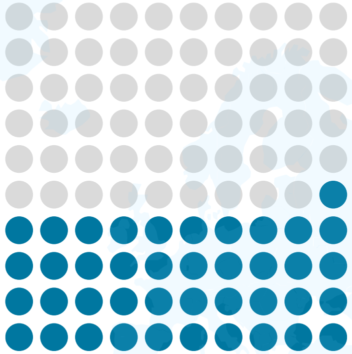
[5] Nikkei Asia (2024). Taiwan chip industry sails overseas amid supply chain shift
https://asia.nikkei.com/Spotlight/Supply-Chain/Taiwan-chip-industry-sails-overseas-amid-supply-chain-shift

Measures taken by tech companies due to a challenging economy



66%

initiated direct cost reduction initiatives (administrative, operational).



41%

Preserved capital and embarked on rethinking ability to retain risk.

Top 3 actions taken by tech companies for 2024

- Reducing limits | reallocating insurance budget between lines of coverage (joint 1st action)
- Narrowing terms, conditions or definition of services
- Switching primary insurers

Marsh

Navigating a right equilibrium between companies and insurers:

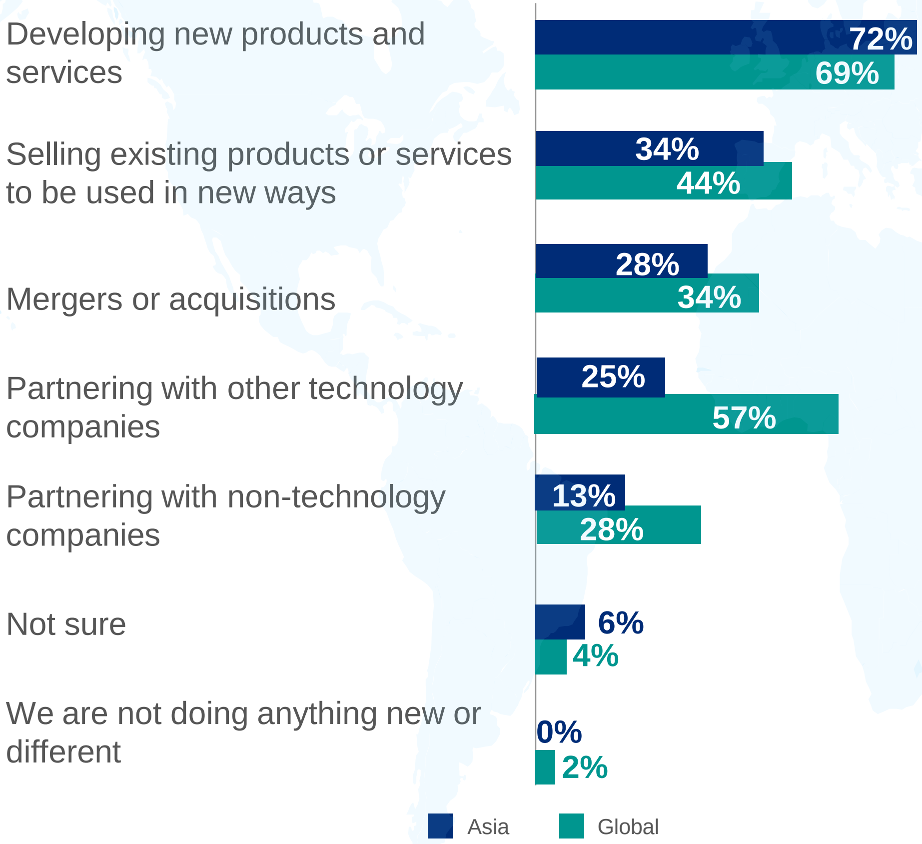
As tech companies expand their footprint into new markets to strive for greater success, they encounter increased exposures and risks. With competing demands on their capital, it is also crucial to allocate resources wisely. On the other hand, insurers are confronted with underwriting concerns and realities as they try to strike a balance between generating a favorable return on equity (ROE) while managing the cost of equity (COE).

As the world's leading risk advisor and insurance broker, Marsh can achieve the best outcomes for your risk mitigation and insurance programs:

- **Optimising capital use** and withstanding market pressures.
- **Strategising the best insurance approach** with multiple sources of risk capital, ensuring flexibility across coverage lines, and identifying the most cost-effective program structure through Risk Finance Optimisation (RFO).
- **Efficient claims process**: Optimise claims processing timelines and outcomes.

Silver lining for tech companies: Developing new products and services to capture new markets remains the top focus

How is your company expanding its products/service offerings?



Product diversification changes risk profiles. In 2024, 72% of tech firms (vs. 82% in 2023) are venturing into new areas, focusing on AI. For example,

- High Performance Computing (HPC) and High Bandwidth Memory (HBM) chips, are two of the new products developed in Asia that enable AI.
- Asia also continues to attract tech investments. Global tech firm Amazon unveiled a US$9 billion investment plan to expand its cloud computing infrastructure in Singapore[6].

As companies diversify their products and services in Asia, risk exposures increase. For instance, adequate liability insurance is necessary to protect against the increased risk of disputes and legal claims.

> **Due diligence remains paramount to tech firms' success. Regardless of product development, infrastructure investments or partnerships, there is a need to proportionately distribute and mitigate risks.**

[6] Amazon to invest $12b to expand cloud computing infrastructure in Singapore
https://www.channelnewsasia.com/watch/amazon-invest-12b-expand-cloud-computing-infrastructure-singapore-4319091

Key takeaways

In today’s fast-changing risk environment, tech firms must continuously refine their risk management strategies to safeguard against technological, commercial and operational threats.

1

Continual risk identification: Ongoing identification of diverse risks is essential.

2

Bespoke risk quantification: Use new approaches and data to quantify emerging risks.

3

Adaptable risk program: Leverage alternative structures and risk capital for flexible risk transfer programs.

4

Expansive stakeholder engagement: Engage all stakeholders, including customers, partners and regulators.

5

Persistent financial discipline: Maintain ongoing diligence to support innovation and growth.

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or re- insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the sole responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position. Insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies. Policy terms, conditions, limits, and exclusions (if any) are subject to individual underwriting review and are subject to change.

A business of Marsh McLennan