QBE Insurance

Strengthening Governance and Resilience in the Age of AI-Driven Threats

By Benny Kiong, Cyber Underwriter - Financial Lines, QBE Malaysia

Agenda

1 **Governance**

2 **Resilience**

3 **Coverage**

QBE Insurance

Governance

Current Situation

No binding AI Legislation, Only Guidance

- **Voluntary guidelines** by MOSTI's AI Governance & Ethics (AIGE) (fairness, transparency, accountability, privacy, safety, inclusiveness, human well-being)[1]

- **Signals of future regulation** by BNM launching AI Governance Framework (2025) together with Asian Institute of Chartered Bankers (AICB)[2]

1 - https://mastic.mosti.gov.my/publication/the-national-guidelines-on-ai-governance-ethics/
2- AICB | Driving Responsible AI Adoption: Introducing the AI Governance…

Problem

- **Future Disruption:** Rushing to comply creates disruption when rules arrive. Lead to exposure to investigations, fines, reputational harm[3]
- **Leaders at risk**: Directors liable if AI misuse causes harm (bias, privacy breach, unsafe automation)
- **Real-world Case Study**: 2024, in Hong Kong, deepfake scammer stole $25 million from a Multi-National Company[4]

3 - Bank Negara Malaysia's Discussion Paper – Artificial Intelligence in The Malaysian Financial Sector – HHQ
4 - Deepfake scammer walks off with $25 million in first-of-its-kind AI heist - Ars Technica

Solution

01

Adopt AIGE principles: Implementation of guidelines as a way of preparedness (setting policies, defining roles, building a risk dictionary)

02

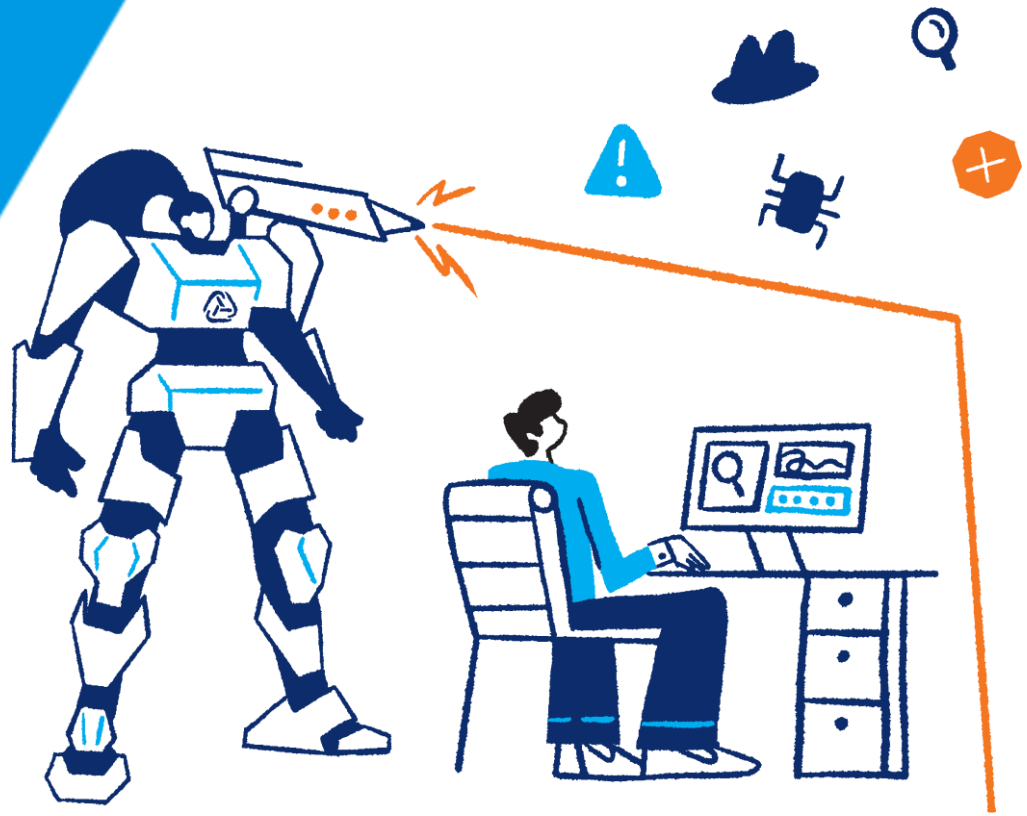
Integrate AI risk into Enterprise Risk Management (ERM): Include AI risks in your regular risk reports and board meetings

03

AI Model Assurance: Check AI systems for mistakes and keep good records

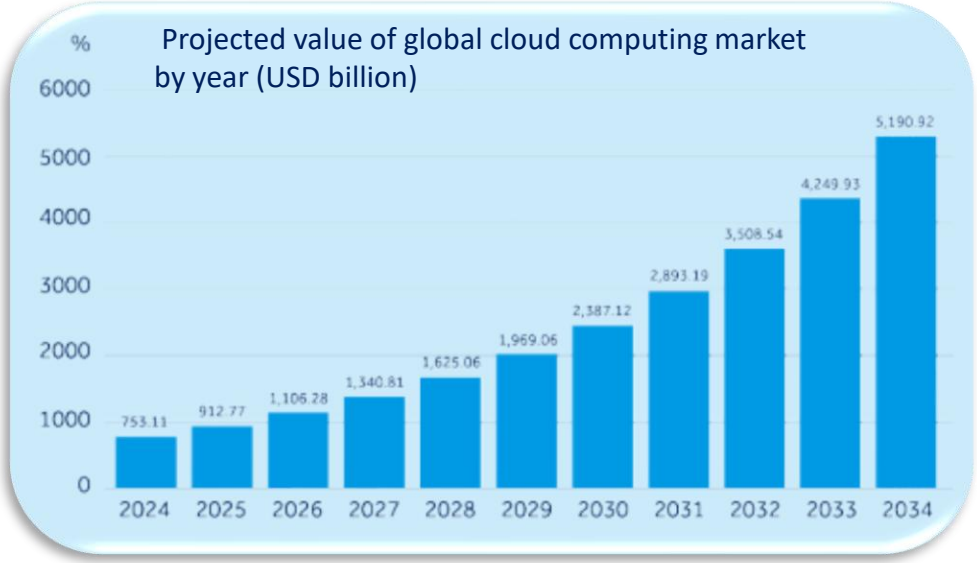
QBE Insurance

Resilience



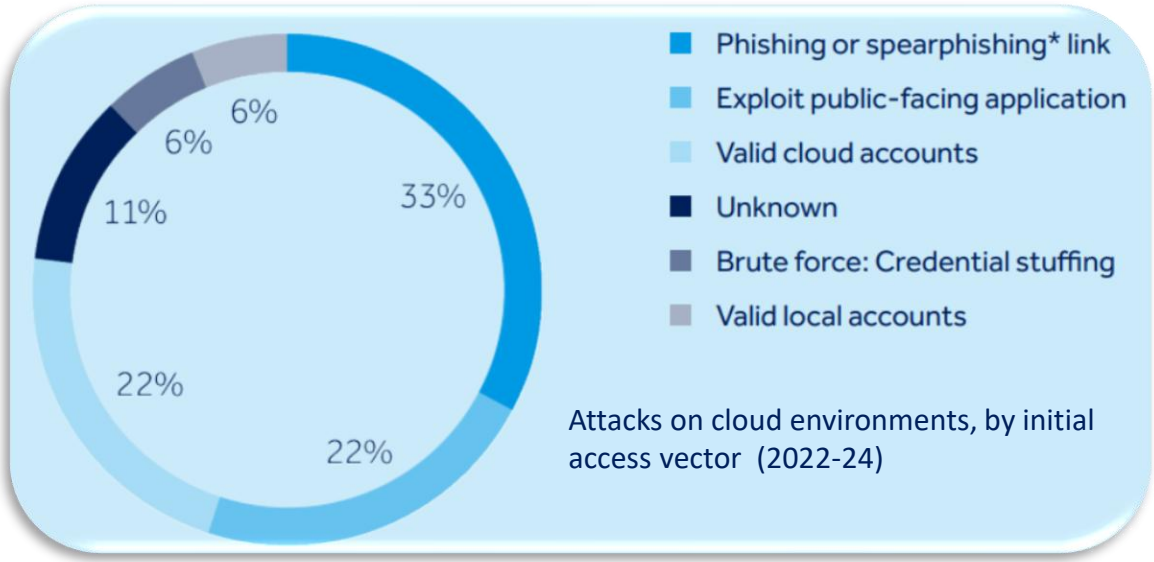
Current Situation

Rapid adoption of cloud computing + AI tools



Source: Precedence Research[5]

Multiple attack vectors



Source: IBM[8]

~$5 Tn

The global market is expected to exceed USD 5 trillion by 2034[6]

High surge adoption reflects in ransomware & AI-assisted fraud trending up, third-party outages disrupt business[7]

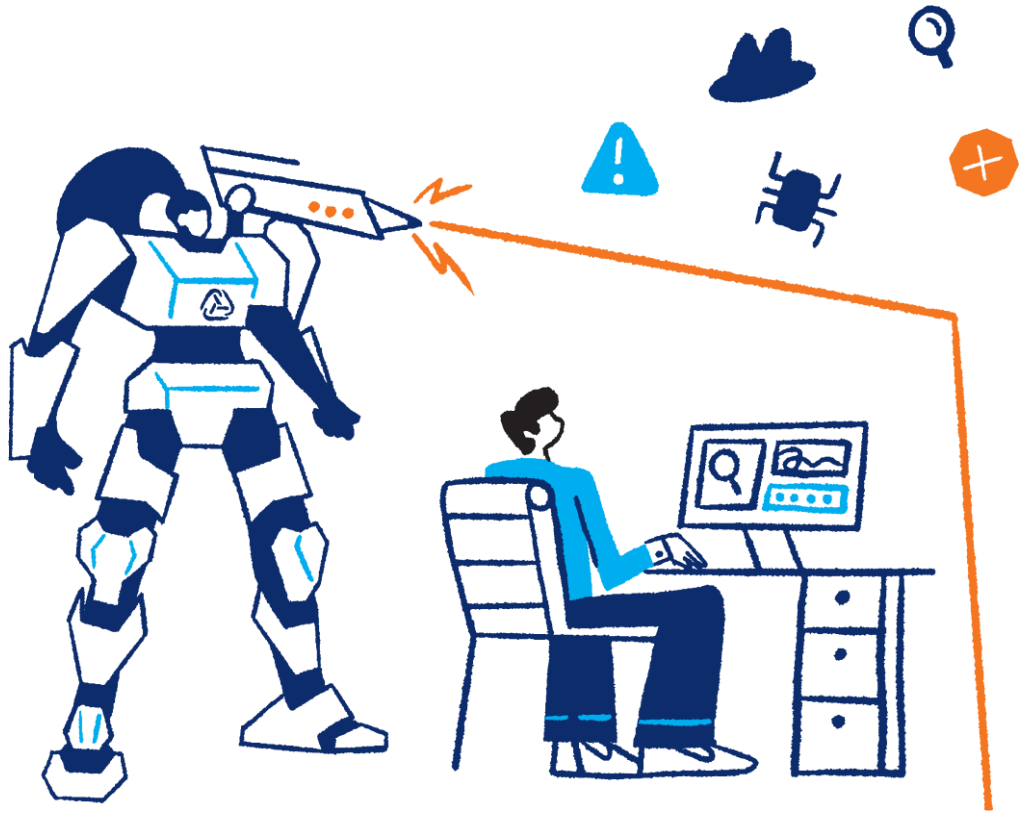
33%

Phishing remains the leading access point for cloud-related incidents, accounting for one-third (33%) of intrusions in 2023 and 2024[9]

6 - precedenceresearch.com/cloud-computing-market
7 - https://www.it-isac.org/post/q1-2025-our-newest-ransomware-report-update
8 - ibm.com/new/announcements/x-force-cloud-threat-landscape
9 - X-Force report reveals top cloud threats: AITM phishing, business email compromise, credential harvesting and theft | IBM

Problem

- **Control Blindspot**: Traditional controls miss AI-driven threats (deepfakes and LLMjacking)[10]
- **Third-Party Vendor Risk**: Operational downtime when vendors fail (cloud/CDN, identity provider, MSP)[11]



10 - https://www.hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
11 - Microsoft says massive Azure outage was caused by DDoS attack

Solution

01

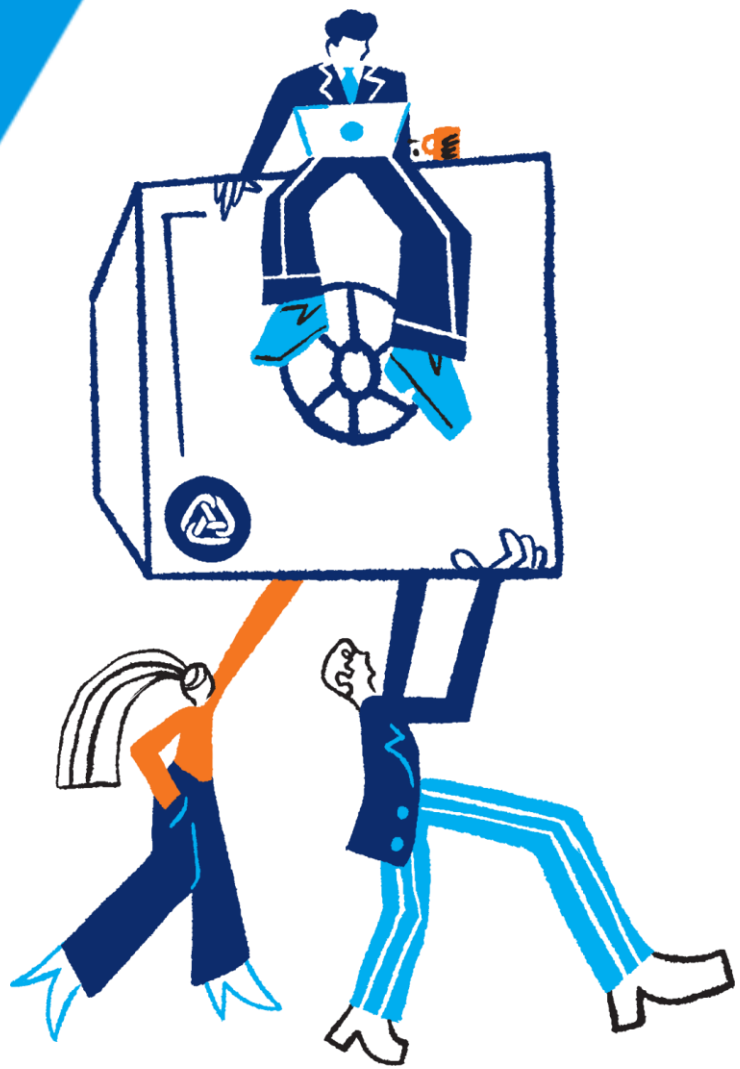
Strengthen Security: Multi-factor authentication (MFA) and user access restriction.

02

Check third-party vendor security: Evaluate third-party security posture to ensure everyone in your supply chain is safe

QBE Insurance

Coverage



Current Situation

- **Regulation Limitations**: PDPA does NOT address AI-specific risks (automated decision making, model bias)

- **Regulation Trajectory**: BNM is signalling future regulation for financial services[12]

12 - Bank Negara Malaysia's Discussion Paper – Artificial Intelligence in The Malaysian Financial Sector - HHQ

Problem

- **Coverage gap**: Traditional cyber policies are often silent on AI-related coverages
- **LLMjacking**: Unauthorised access to LLM accounts can drive up API usage fees, degrade model performance causing financial loss[13]
- **Proactive risk management**: Without tabletop exercises and threat intelligence, coverage gaps may go unnoticed

13 - Cybercriminals are stealing AI power, and you might be the one paying for it | Cybernews

Solution

01

QCyberProtect: AI is not “excluded”. It’s just not mentioned specifically

- **AI Regulatory Proceeding Coverage**: Defense costs + regulatory damages for AI regulatory proceedings
- **LLMjacking Coverage**: Reimburses increased service/ usage charges & retraining costs after an LLMjacking event

02

Complementary Services:

QBE in-house client services[14]

Examples:

- Tabletop Exercise
- Threat Intelligence Webinars
- Etc.

14 - https://www.qbe.com/cyber/cyber-services

QBE Insurance

Takeaways

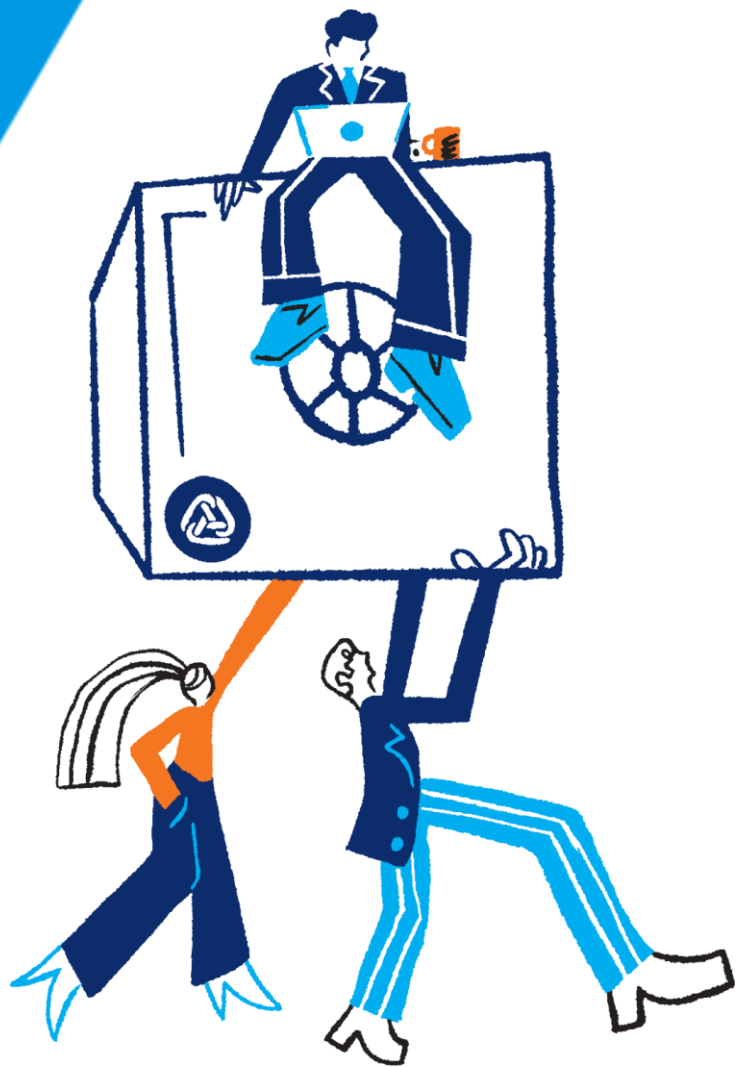
Recognise the gap and prepare for the future

Integrate AI risk into governance and ERM

Strengthen resilience with good security controls and vendor risk management

Examine cyber coverage for silent AI gaps

Use QBE Cyber Services to stay ahead of the curve



It's cyber insurance
powered by real people.

Thank you!