Governance, Resilience & Insurability: What Risk Managers Need to Know About Cyber Insurance in the AI Era

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

Agenda

AI Adoption & Governance Gap

AI Is Moving Beyond Experimentation

AI is no longer just a technology experiment. It is becoming part of the business environment.

- Entering day-to-day operations
- Embedded into business tools
- Supporting decision making
- Used across HR, legal, risk and compliance
- Increasingly delivered through third party platforms

World Economic Forum, Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards, January 2025.

Malaysia’s AI Governance Journey

Current Landscape

- MOSTI launched the National Guidelines on AI Governance & Ethics (AIGE) in 2024
- AIGE remains principles-based and voluntary.
- National AI Office established as a central coordinating body.
- Proposed AI Governance Bill under public consultation.
- Malaysia's AI governance framework remains largely principles-based today but regulatory expectations continue to evolve.

Organisations should prepare before regulation becomes more prescriptive.

MOSTI AIGE; UNESCO Malaysia AI Governance Observatory; AICB AI Governance Framework announcement

Questions Boards Should be Asking

- Who owns AI risk?
- Where is AI being used?
- What data is exposed?
- What happens if AI fails?
- Are we comfortable explaining our AI governance to regulators, customers and insurers?

AI Is Not Just an IT Risk

AI risk requires involvement from:

- Board / Senior Management
- Risk Management
- Cybersecurity
- Legal and Compliance
- HR
- Procurement
- Business Units
- Internal Audit

AI governance needs to sit within enterprise risk management, not only within IT.

World Economic Forum, Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards, January 2025

What Underwriters Are Starting To Ask About AI

Governance
- AI owner identified?
- AI committee in place?
- Board oversight?

Human Oversight
- Human review?
- Override capability?

Risk Management
- AI risk assessment?
- AI system classification?

Documentation
- Model documentation?
- Audit trail maintained?

Data Governance Questions

- What data is used by AI?
- Is sensitive data uploaded into public AI tools?
- Is training data reliable?
- Are bias controls in place?
- Are outputs reviewed?
- Are affected individuals informed?

AI governance is also data governance.

Governance Blind Spots

- Shadow AI
- No AI inventory
- Unapproved public AI tools
- No AI acceptable use policy
- Limited board visibility

You cannot govern what you cannot see.

When Governance Does Not Keep Pace

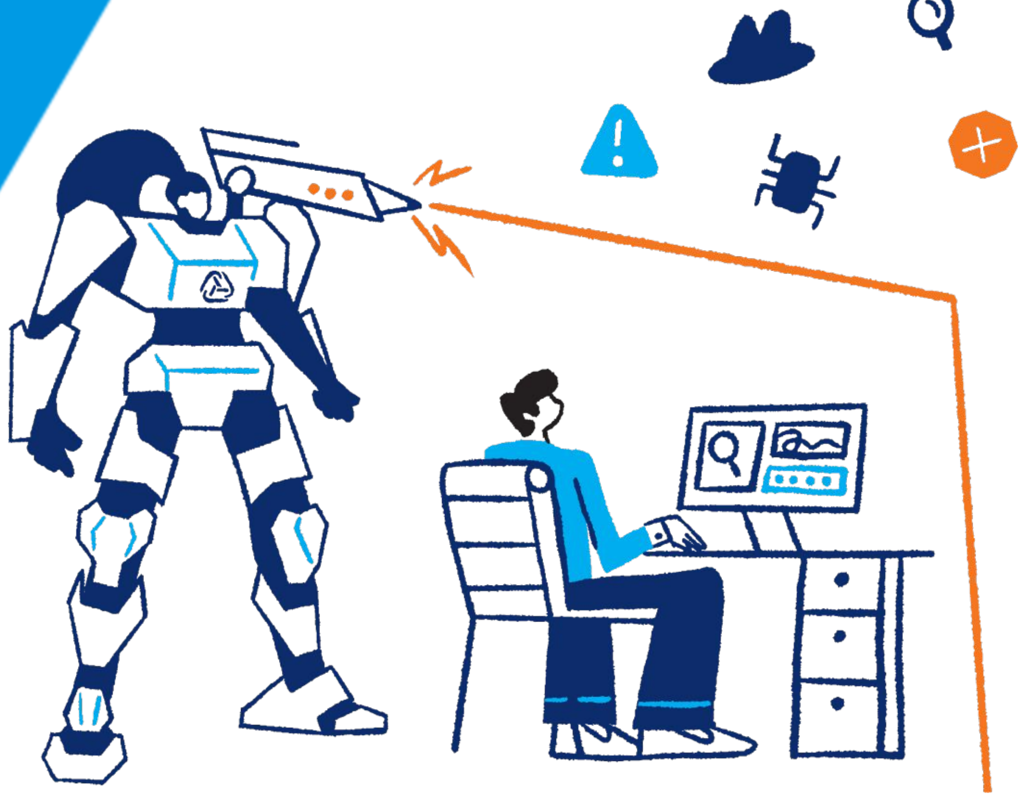
Potential consequences:

- Financial loss
- Regulatory scrutiny
- Privacy exposure
- Reputational damage
- Operational disruption
- Senior management accountability

Real-world Case Study: 2024 Hong Kong deepfake fraud involving reported loss of USD25 million.

Deepfake scammer walks off with $25 million in first-of-its-kind AI heist - Ars Technica

Cyber Resilience in the AI Era



AI Changes The Cyber Risk Landscape

AI affects cyber risk in three ways

Threat actors use AI

Defenders use AI

AI systems need protection

The issue is not only “AI as a threat”. It is also “AI as part of the business environment”.

How Threat Actors Use GenAI

- More convincing phishing
- Deepfake impersonation
- Fake identities
- Malware development
- Vulnerability exploitation
- Disinformation content

Faster, cheaper, more scalable and more convincing.

AI Creates New Assets To Protect

AI systems involve

- Input data
- Training data
- AI models
- APIs and interfaces
- Monitoring tools
- Output data
- Business applications

Potential risks

- Prompt injection
- Data poisoning
- Model manipulation
- Data leakage

Resilience Gaps Risk Managers Should Watch

- Deepfake fraud exposure
- Prompt injection risks
- Cloud dependency
- AI vendor dependency
- Business interruption exposure
- Weak incident response planning
- Limited visibility over critical vendors

AI resilience is not only about protecting the model. It is about protecting the business processes that rely on it.

Controls That Improve Resilience

Foundational Controls

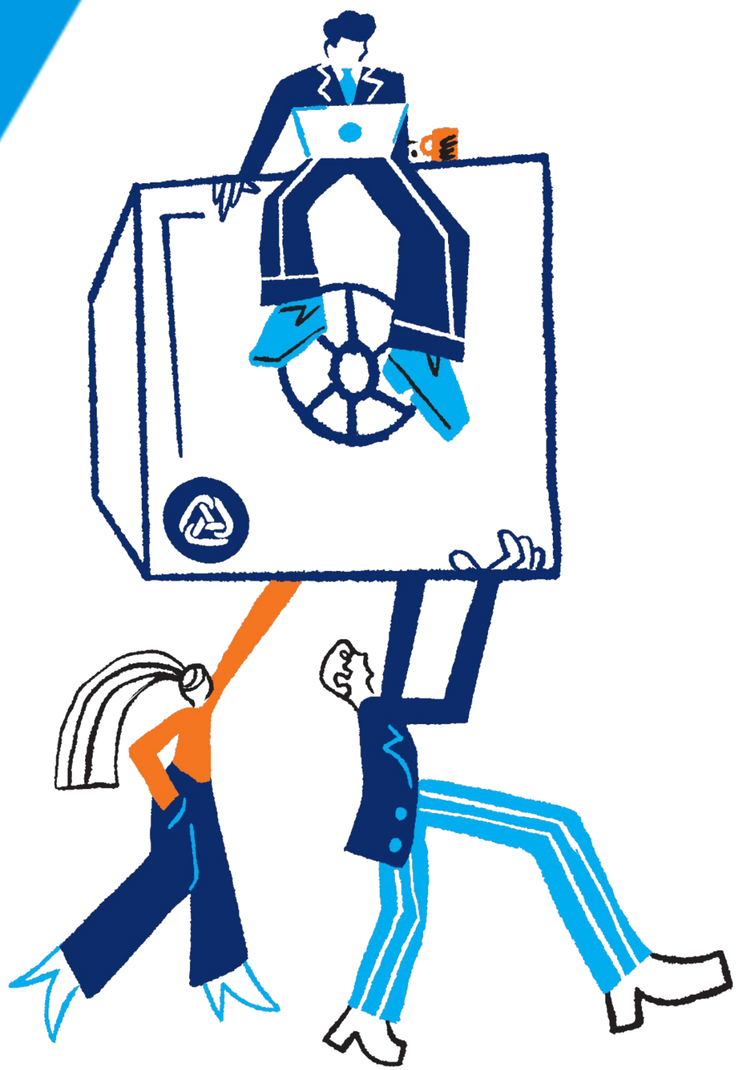
- MFA
- EDR
- Backups
- Patch management
- Privileged access management
- Incident response plan
- Vendor risk assessment

AI-Specific Controls

- AI inventory
- AI usage policy
- Human review
- AI monitoring
- AI vendor assessment

AI does not replace cyber hygiene. AI makes cyber hygiene more important.

Cyber Insurability & Coverage Considerations



What Makes an Organisation Insurable?

Governance

- AI ownership
- AI policy
- Board oversight

Visibility

- AI inventory
- Shadow AI controls
- Vendor mapping

Resilience

- MFA
- EDR
- Tested backups
- Incident response

Assurance

- Documentation
- Monitoring
- Human oversight

Good governance improves insurability.

Same Industry, Different Outcome

Organisation A

- MFA and EDR implemented
- AI use cases documented
- Backups tested
- Vendors assessed
- Incident response tested
- Board visibility

Question: What would be the view from the Underwriting perspective?

Likely underwriting view: Greater confidence in resilience and recovery capability.

Same Industry, Different Outcome

Organisation B

- Partial / No MFA
- No clear AI owner
- Shadow AI usage
- Untested backups
- Limited vendor oversight
- Cyber treated as IT issue

Question: What would be the view from the Underwriting perspective?

Likely underwriting view: Higher uncertainty around controls, resilience and potential loss impact.

Coverage Questions Risk Managers Should Ask

- Does our cyber policy respond to AI-related incidents?
- Are regulatory investigations covered?
- Are cloud and AI vendors considered?
- Could AI misuse trigger fraud or privacy issues?
- Are increased usage charges or retraining costs addressed?
- Are cyber limits still adequate?

Coverage should be reviewed before an incident, not during one.

Insurance Is One Layer Of Resilience

Cyber insurance can support:

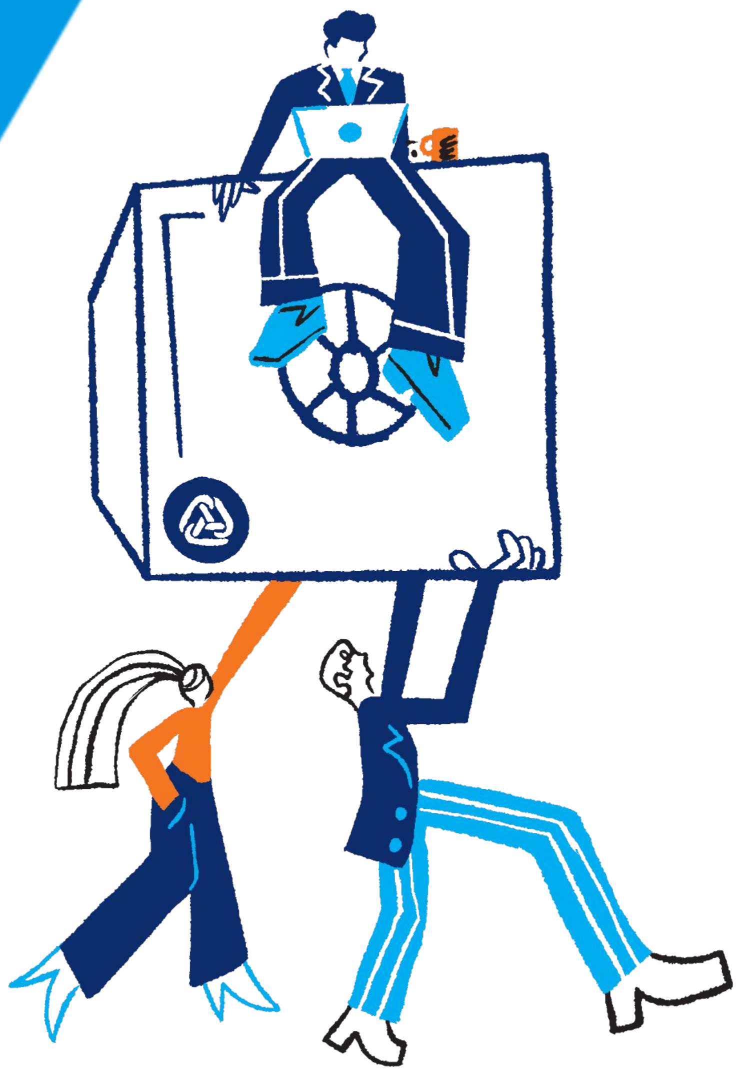
- Incident response
- Forensics
- Crisis communications
- Data restoration
- Business interruption
- Liability protection
- Regulatory defence costs
- Risk management services

Insurance complements governance and controls. It does not replace them.

Key Takeaways

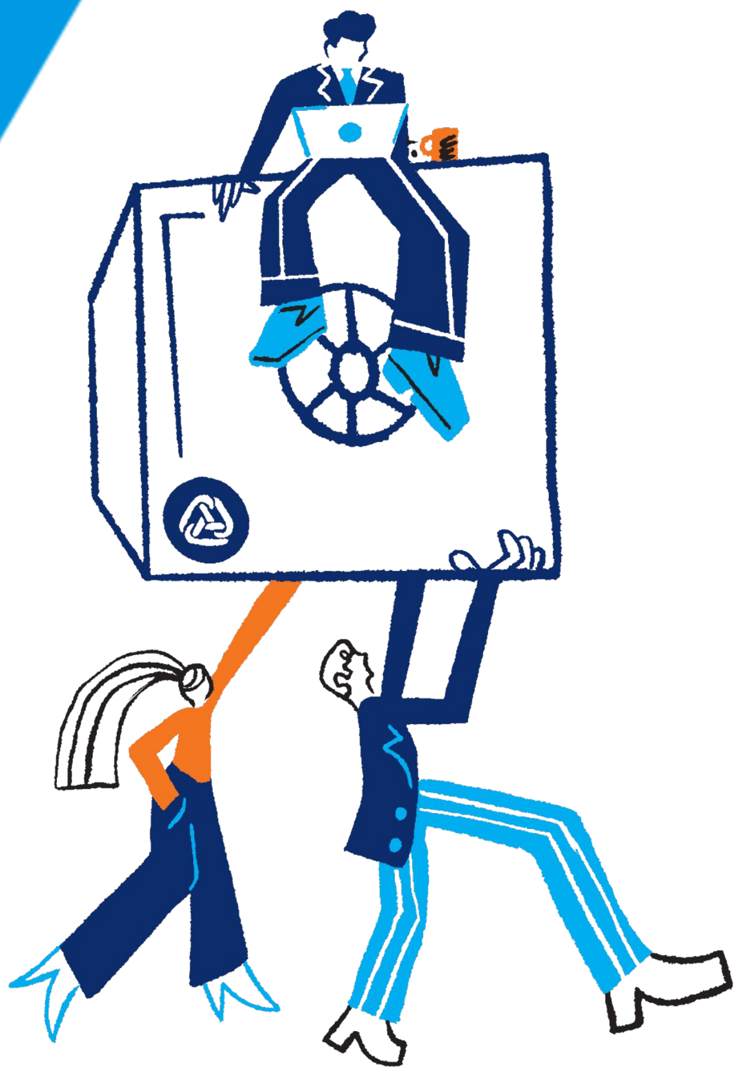
- AI adoption is accelerating
- Governance must keep pace
- AI is an enterprise risk
- Resilience improves insurability
- Coverage should be reviewed early

Governed. Resilient. Insurable.



Three Questions Every Risk Manager Should Ask

- **Are we governed?**
- **Are we resilient?**
- **Are we insurable?**



It's cyber insurance
powered by real people.

Thank you!