CLYDE&CO

The Cyber Insurance EvThe Cyber Insurance Evolution?

Drafting Policies for AI Risks

Nick Gibbons, Legal Director

AI Is Not Cyber 2.0

- Cyber policies were designed to address system compromise and data breaches.
- AI introduces risks that arise without hacking or unauthorised access.
- Hallucinations, bias, automation failures and autonomous decisions create new exposures.
- Existing policy language often assumes human conduct and human judgement.
- Insurers face growing "silent AI" exposure across multiple product lines.
- Traditional cyber controls remain necessary, but they are no longer sufficient.

Key Questions

- Why is AI risk different from cyber risk?
- What new governance and controls are required?
- How should insurers underwrite AI risk?
- How must policy wordings evolve?

Why AI Risk Is Different

- AI creates risks even where no system is hacked.
- AI can generate incorrect decisions, advice and outputs.
- Traditional cyber controls protect systems, not machine behaviour.
- AI can be manipulated through prompts rather than network intrusion.
- Privacy frameworks focus primarily on personal data.
- AI risks extend to intellectual property, commercial information and business logic.
- AI introduces decision risk as well as information risk

Existing Cyber Controls Are Not Enough

- Firewalls cannot prevent hallucinations.
- MFA does not stop biased AI decisions.
- Encryption cannot prevent inaccurate recommendations.
- Traditional penetration tests rarely assess AI behaviour.
- AI can disclose data without technical compromise.
- Organisations need AI-specific governance controls in addition to cybersecurity.
- Good cybersecurity does not guarantee safe AI.[1]

AI Creates New Governance Requirements

- AI influences decisions affecting customers, employees and third parties.
- Boards must understand and oversee AI risk.
- Clear ownership and accountability are essential.
- AI risk affects legal, compliance, operational and reputational exposures.
- AI deployments should follow formal approval processes.
- AI risks should be incorporated into enterprise risk management.
- AI is an enterprise risk issue, not simply an IT issue.

New Policies Businesses Need

- AI Acceptable Use Policy.
- AI Data Handling and Classification Policy.
- AI Procurement and Vendor Assessment Policy.
- AI Incident Response Policy.
- AI Development and Testing Policy.
- AI Monitoring and Audit Policy.
- **Key Message:** Existing cyber and privacy policies do not adequately govern AI

Training Becomes Critical

- Staff must understand approved AI tools.
- Employees need training on hallucinations and reliability risks.
- Training should cover deepfakes and AI-enabled fraud.
- Staff must understand confidentiality restrictions.
- Employees should recognise prompt injection risks.
- Managers need additional training on AI-supported decisions.
- Most AI failures begin with people, not technology

AI Requires New Technical Controls

- Approved enterprise AI platforms only.
- Restrictions on public AI and personal accounts.
- Prompt filtering and AI security gateways.
- Monitoring of AI inputs and outputs.
- Segregation of sensitive data sources.
- Comprehensive logging and audit trails.
- **:** AI requires dedicated technical controls beyond traditional cyber security.[1]

AI Risk Assessments

- Assess confidentiality and data leakage risks.
- Assess potential for inaccurate outputs.
- Assess bias and discrimination risks.
- Assess regulatory and legal compliance risks.
- Assess operational resilience risks.
- Assess potential customer and business harm.
- Every significant AI deployment should undergo an AI Impact Assessment.

AI Systems Must Be Tested

- Prompt injection testing.
- Hallucination testing.
- Bias and fairness testing.
- Accuracy and consistency testing.
- Independent assurance and audit reviews.
- Controls that are not tested cannot be trusted.

Roles and Responsibilities

- Board sets AI strategy and risk appetite.
- Legal manages liability and regulatory exposure.
- Compliance monitors regulatory obligations.
- Risk teams oversee enterprise AI risk.
- IT deploys and supports AI solutions.
- Information Security protects infrastructure and data.
- Effective AI governance requires a multidisciplinary approach

What Good Looks Like

- Clear Board accountability.
- Dedicated AI governance framework.
- Comprehensive policies and procedures.
- Mandatory staff training.
- AI-specific technical safeguards.
- Continuous testing, monitoring and audit.

Why Existing Insurance Policies Are Struggling

- Most policy wordings were drafted before widespread AI adoption.
- Policies generally assume human decision-making.
- AI introduces autonomous and semi-autonomous actions.
- Existing cyber definitions focus on network compromise.
- Many AI losses occur without a cyberattack.
- Coverage intent and policy language are increasingly diverging.
- **Insurance products were designed for cyber risk, not machine decision-making risk.**

The Rise of Silent AI Exposure

- Many insureds are already using AI.
- Proposal forms rarely ask meaningful AI questions.
- Policies often contain no AI-specific definitions.
- Traditional PI policies may inadvertently cover AI failures.
- D&O, EPL and Liability policies may respond unexpectedly.
- Insurers may be carrying unquantified AI exposure.
- **Silent AI may become the successor to silent cyber.**

New Categories of AI Claims

- Hallucinated professional advice.
- AI-assisted underwriting errors.
- AI-generated employment discrimination.
- Deepfake payment fraud.
- AI-enabled intellectual property infringement.
- Autonomous decision-making causing customer loss
- **Future AI claims may look very different from traditional cyber claims.**

How Underwriting Must Change

- Assess AI governance, not just cybersecurity.
- Evaluate staff training and oversight.
- Review AI policies and procedures.
- Assess AI vendor management processes.
- Understand AI-enabled business activities.
- Examine testing, monitoring and audit frameworks.
- **Future AI underwriting will focus as much on governance as technology.**

The Future AI Insurance Framework

- Cyber insurance protects systems.
- Privacy insurance protects personal data.
- PI insurance protects professional judgement.
- AI insurance should address machine behaviour.
- Governance standards should influence terms and pricing.
- Insurance products must evolve alongside AI adoption.
- **The next generation of insurance policies will not simply insure technology. They will insure the governance, supervision and behaviour of intelligent systems.**

ANY QUESTIONS?

What Policy Drafters Need to Consider

- Clear definitions of AI systems.
- Treatment of autonomous decisions.
- AI-specific exclusions and carve-backs.
- Coverage for hallucinations and errors.
- Responsibility for third-party AI providers.
- Regulatory investigation and defence cost provisions
- **Policies need precise AI language to avoid uncertainty and coverage disputes.**

Final Takeaway

- **Cybersecurity protects systems.**
- **Privacy governance protects personal data.**
- **AI governance protects machine behaviour, decisions and outputs.**

- **Organisations now need all three operating together.**