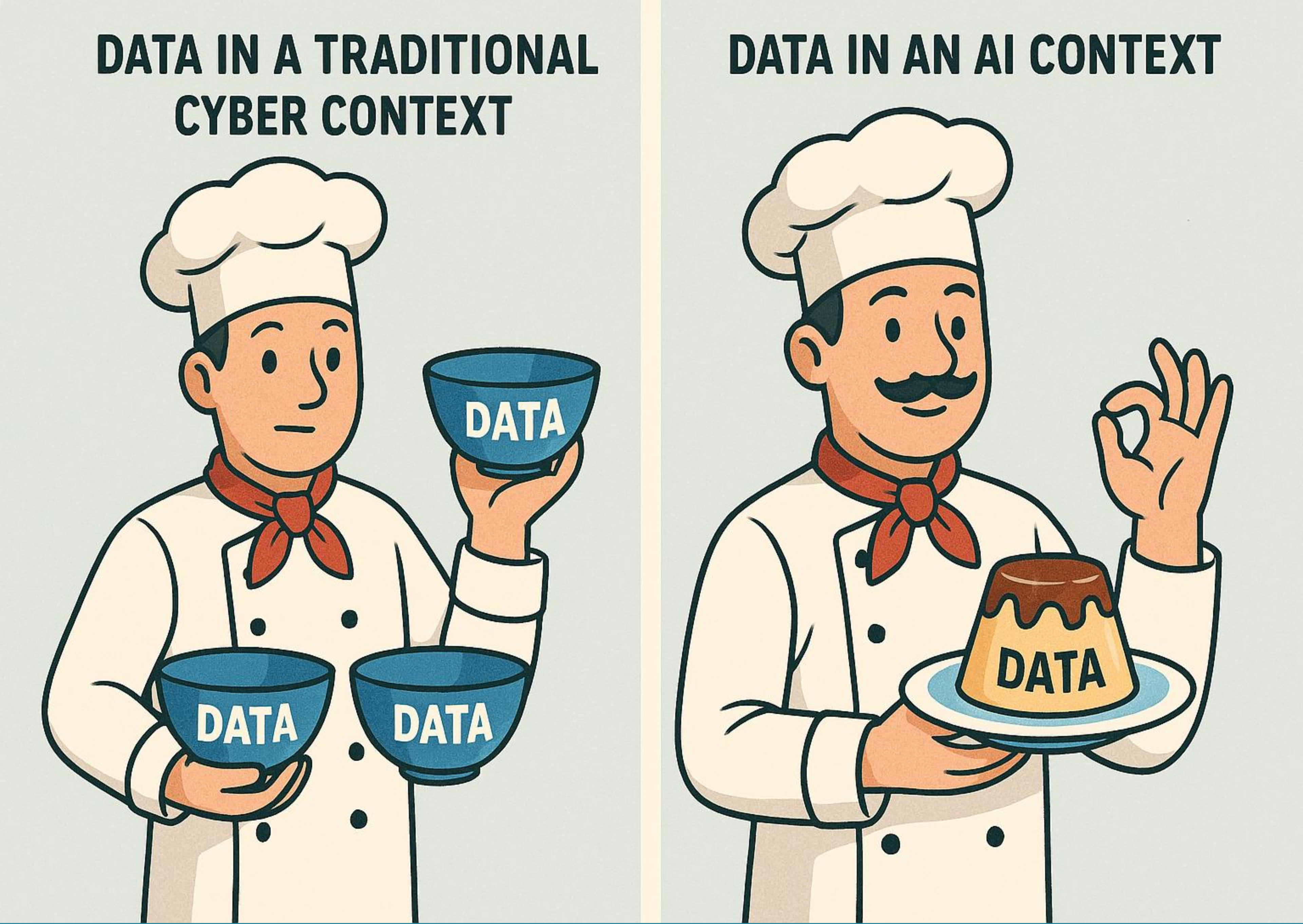
CLYDE&CO

The legal challenges presented by AI

Nick Gibbons, Legal Director


DATA IN A TRADITIONAL CYBER CONTEXT
DATA
DATA
DATA
DATA IN AN AI CONTEXT
DATA

AI and Cyber : Understanding the Distinction

- AI information security and cyber security are not synonymous.

- Cyber deals with networks and internet-connected systems

- AI solutions are the brain of an organisation that aggregates and processes data and makes decisions

- AI introduces new classes of vulnerabilities and broader categories of data at risk.

-

Why every business is now an AI Business

Sectors using AI extensively include:

- Healthcare
- Law
- IT & Software
- Finance
- Marketing
- Creative professions
- Education & Research
- Engineering & manufacturing

Cybercrime Becomes a Business

From High Skill / Low Volume → Low Skill / High Volume

Content:

- Automated cybercrime tools.
- Mass-scale attacks with extremely low skill.
- Fake websites, phishing, deepfakes, domain spoofing.

AI-Specific Attacks

Beyond Traditional Cyber Threats

Key AI attack vectors include:

- Adversarial attacks
- Model inversion
- Data poisoning
- Prompt injection
- Model extraction
- Backdoor attacks
- Membership inference
- Gradient leakage
- Jailbreaking
- Synthetic identity generation

Legal Framework Overview

Existing Law Already Applies to AI

Content:

- GDPR
- UK NIS Regulations
- DORA (EU)
- NIS2
- EU AI Act

UK common law (confidentiality, negligence, misrepresentation)

Why AI Risk Now Extends Beyond Personal Data

- GDPR limited to personal data.
- New rules cover every type of data.
- More specific

. technical measures.

. Auditing requirements.

. More rigorous sanctions

Why Enterprise AI Solutions Are Safer Than Public AI (e.g., ChatGPT)

- Data isolation & no-training guarantees:
- Centralised, policy-enforced access control
- Automatic redaction & secret scanning:
- Zero Trust & segmentation
- Governance & oversight

Contractual Exposure of AI Vendors

AI vendors may face liability for:

- **Negligent misstatement, negligent misrepresentation, or failure of the AI to perform as described.**

- **Breach of confidence or misuse of information where the system leaks, reconstructs, or exposes data.**

- **Infringement of IP rights (copyright, design, trademark) generated or enabled**
- **by the system.**

What Hackers Can Do During AI Solution Implementation

- Compromise credentials before go-live
- Exploit overshared data in staging environments
- Poison training data or vector indexes
- Prompt injection during development
- Man-in-the-middle during API/configuration setup
- Exploit unpatched or misconfigured environments

AI in Insurance Context
Why AI Risk > Cyber Risk

AI risk includes:

- Breach of contract
- Negligence
- Misstatement/misrepresentation
- Breach of confidence
- IP infringement
- Defamation
- Breach of professional duty

Insurance Blind Spots
“Secret” AI Exposure

- AI is already embedded in business operations.
- Businesses often rely on AI outputs without verifying accuracy.
- Exclusion clauses for cyber/hacking usually do not exclude AI misuse.
- Unreasonable reliance on AI may create negligence liability.
- Very few policies include AI-specific exclusions

Any Questions ?