Chapter 4: How AI is changing cyber risk

The email looked perfect

Imagine a client receives an email from their Managing Director.

- → The tone sounds right
- → The spelling is perfect
- → The request seems reasonable
- → There are no obvious warning signs

The problem?

The Managing Director never sent it.

Welcome to the AI era.

> 68% of SMEs say AI makes them more likely to purchase cyber insurance.

AI isn't creating new cyber threats

It's making existing threats better.

Cybercriminals have always used phishing emails, fake invoices, impersonation and fraud.

AI simply helps them do it faster, at greater scale and with fewer mistakes.

Client says / Reality says

Client says:
"I'd spot a phishing email."

Reality says:
Modern phishing attacks don't always look suspicious. AI can help attackers create highly convincing messages that closely mimic genuine communications.

Seeing is no longer believing

AI isn't limited to emails.

It can generate:

- ✓ Voice messages
- ✓ Phone calls
- ✓ Videos
- ✓ Images

> 79% of SMEs say AI is making cyberattacks more sophisticated and harder to prevent.

In one widely reported example, an employee was allegedly tricked into transferring millions after participating in a video call populated entirely by AI-generated deepfakes.

Broker conversation starter

> "How would your team verify a payment request from a senior executive if the email, voice and video all looked genuine?"

Could AI take over your mailbox?

A growing area of risk involves AI agents that can take actions rather than simply generate content. Businesses are increasingly connecting AI systems to email, knowledge bases, cloud platforms and operational workflows. While this can improve efficiency, it can also create new governance challenges if AI systems are granted excessive permissions or allowed to act without appropriate oversight.

A simple example

An AI-powered mailbox assistant might be asked to:

- Read incoming emails
- Route requests automatically
- Draft responses
- Trigger workflows

If a malicious email contains hidden instructions designed to influence how the AI behaves, known as a prompt injection attack, the AI could potentially be manipulated into taking actions that were never intended.

AI creates opportunity as well as risk

Businesses are increasingly using AI to draft content, analyse information, automate tasks and support decision-making. In many organisations, adoption is happening faster than governance.

Key questions include:

- → **What information is being shared?** Employees may upload customer data, contracts, financial information and other sensitive material into AI tools.
- → **Who can access AI tools?** Many businesses have limited visibility over which platforms are being used and by whom.
- → **What decisions can AI influence?** AI can support recommendations, content creation and operational decisions, but accountability remains with the business.
- → **How is its use monitored?** Governance, oversight and employee guidance often lag behind adoption.

AI and Data Exposure

A weak AI policy is not a claim in itself.

However, the consequences can quickly become significant where AI use contributes to a:

- Data exposure
- Privacy incident
- Regulatory investigation
- Reputational issue

Employees may upload sensitive customer information, contracts or financial data into external AI platforms. Businesses may also face allegations that AI-generated content reproduces or infringes third-party intellectual property.

In some cases, organisations may need to investigate:

- What information was shared
- Whether it was retained by the platform
- Whether any legal or regulatory obligations arise

Insurance relevance

While AI introduces new technology risks, many of the resulting losses fall into familiar cyber insurance categories such as Incident Response Services, Privacy Liability and Business Interruption.

Depending on the circumstances, AI-related issues around copyright infringement may also involve: Multimedia Liability - if arranged as a policy extension or specific cover.

Key takeaway



AI doesn't change the fundamentals of cyber risk. It amplifies them.

Attackers still exploit trust, people still make decisions and sensitive information still needs to be protected.

Businesses should understand:

- What information is being shared with AI tools and whether sensitive data, contracts or customer information could be exposed.
- Who can access AI platforms, what systems they can connect to and how their use is governed.
- How AI-generated content is reviewed before use and whether appropriate controls exist to manage intellectual property, privacy and regulatory risks.

The technology may be evolving, but the need for good governance, oversight and cyber resilience remains the same.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Can a Single Email Take Over Your AI Mailbox?
Explores how AI-powered tools can introduce new risks if malicious instructions are hidden within content.

Dabbling with Deepfakes
A practical look at AI-generated voice and video impersonation and what businesses can do about it.

Risk Versus Reward: Using AI in Business
A broker-friendly introduction to AI, its benefits and the emerging risks organisations should understand.

The Generational Shift in Cyber Extortion
How AI is helping threat actors scale attacks and evolve extortion tactics.