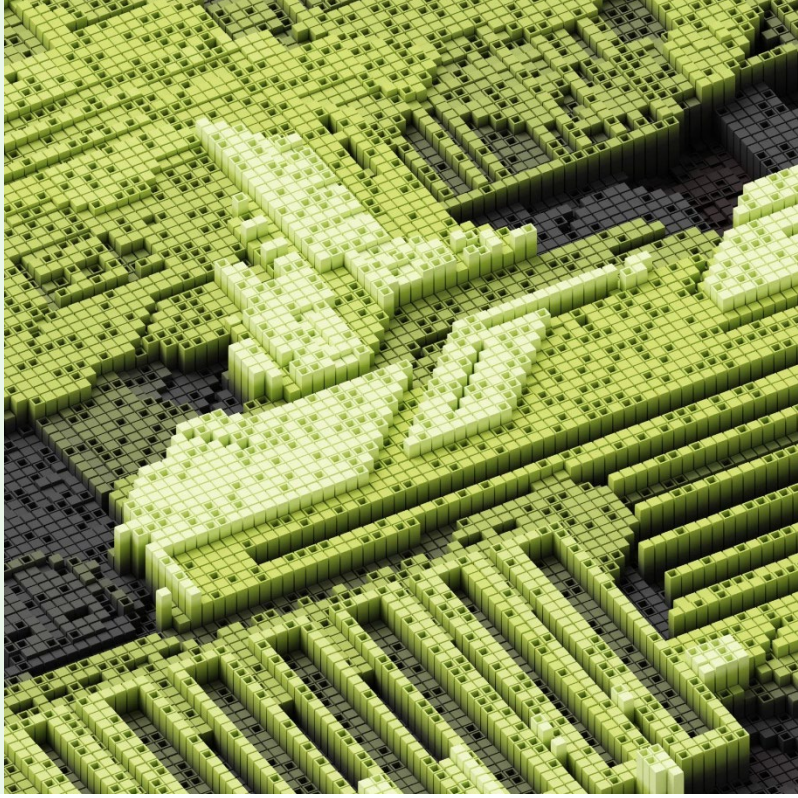
Clifford Chance

BRIEFING

What Mythos means for your business

Action to take now

21 April 2026



A practical checklist for boards and senior leaders on AI-enabled cyber threats, resilience and controls

AI's cyber capabilities are advancing fast. AI-related cybersecurity risks – and expectations of preparedness – are rising. Recent limited or restricted releases of new AI models with advanced cyber capabilities highlight AI's exceptional potential to bolster cyber defence, as well as the risk of strengthened cyber-attacks if misused.

AI is reshaping cyber defence and cyber risks

Prominent AI developers have restricted access to their latest, most cyber-capable AI models – either previewing a model to only a limited set of trusted partners or allowing only identity-verified access at this stage – stating that these AI models have exceptional capacity to autonomously identify and exploit previously unknown cyber vulnerabilities at speed and scale. These capabilities could greatly assist organisations in identifying and addressing cyber vulnerabilities that were previously undetected and significantly boost their cyber defence capabilities. At the same time, the AI developers have voiced concerns that such capabilities could be misused to accelerate cyberattacks.

This strategy of granting access only to a closed network of trusted partners is intended to give defenders a head start and reduce the risk of misuse – underscoring a focus not only on model capability but also on trust and responsibility.

What this means for businesses

The emerging cyber capabilities of AI models are bringing a significant shift in the threat landscape, including:

(1) a possible step-change in cyber-attack volume and sophistication as more actors (including non-experts) have the capability to detect and exploit cyber vulnerabilities effectively;

(2) capacity for automated exploit development leading to compressed time frames between vulnerability discovery and exploitation – with the time to exploit following discovery potentially being significantly shorter than the time frame needed to patch/fix; and

(3) AI-accelerated activity once attackers are within an organisation's systems, reducing the time available for investigation, escalation and response.

This will raise the bar for what is needed for effective cybersecurity and operational resilience in practical terms and will impact certain legal and contractual requirements, as well as regulatory expectations, regarding appropriate controls. Regulators are concerned by the increased cyber risk posed by advanced AI, particularly for legacy systems, and are actively considering its implications for financial stability, market resilience and critical infrastructure.

This is a board-level priority, requiring robust oversight of controls, preparedness for AI-specific threats, and clearly defined roles within well-tested incident response plans.

What to do now: a practical checklist

Boards and senior managers need to understand their organisations' cybersecurity and operational resilience position, determine the actions to be taken to address AI-accelerated cyber risk, and be ready to explain these to regulators and other stakeholders. These steps should include:

1. **Reviewing core cyber safeguards**
    - **Review vulnerability management**: this should include confirming that you have a defensible, risk-prioritised penetration testing, patching and remediation approach aligned to regulator expectations.
    - **Refresh mapping of critical systems and data**: make sure you have an up-to-date picture of your most important IT systems and data, identify key weak points (such as legacy/unsupported software and accounts with "admin" power) and address the most urgent risks first.
    - **Contain the impact of cyber-attacks**: validate network segmentation and access controls around critical systems and sensitive data to limit the ability for hackers to move laterally across systems. Strengthen identity controls, particularly for privileged accounts.
2. **Updating preparedness plans**
    - **Add AI-enabled attacker assumptions into enterprise threat modelling and re-run resilience scenarios for critical services**: anticipate faster detection and exploitation of vulnerabilities, credible social engineering at scale and simultaneous attacks across suppliers.
    - **Ensure that your organisation has actionable, cross-functional incident response plans** that can help you to react effectively and to meet (potentially short) regulatory notification deadlines. Include clear escalation and decision trees (including for ransomware payment), a cross-regime notification matrix and a playbook for communications with regulators, staff, customers, the media, the stock market and other stakeholders.

Factor in contractual commitments and insurer requirements. Check that physical copies of preparedness plans and other relevant documentation exist and are easily accessible by key stakeholders.

- **Test and rehearse plans**: run regular tabletop incident response drills, ideally including critical suppliers.
- **Confirm backup and restoration readiness** and test restoration of your IT systems under realistic constraints. Identify the communication channels your organisation will use to respond to a cyber incident in the event that your normal systems are offline.

3. **Strengthening detection and response capability**
   - **Modernise your cyber defence approach**: ensure that your tools and processes can spot unusual behaviour quickly, prioritise identity and access risks and trigger rapid, pre-approved containment action. Cyber defences need to be able to react with AI speed for compressed attack timelines.
   - **Close critical gaps with interim safeguards**: where improvements will take time, put temporary controls in place to reduce risk (for example, tighter access rules and additional monitoring).
   - **Use trusted intelligence to stay ahead**: monitor credible insights from organisations testing frontier models and align with your security partners on how evolving AI capabilities change attacker tactics and defensive priorities.
4. **Treating third-party and supply chain cyber risk as critical**
   - **Build a risk-ranked supplier list (starting with critical services, sensitive data access and concentration risk)**: examine what you know about suppliers' cybersecurity and operational resilience controls and whether you have information or audit rights that you wish to exercise. Is there a strategy to prevent single points of failure? Are there critical systems without effective back-up or other deficiencies? Is there appropriate supply chain diversification to help manage the risks of system unavailability?
   - **Check your contractual clauses, starting with critical suppliers**: when must suppliers notify you, what cooperation is required, what evidence/logs are available and do these align with *your* regulatory obligations? What flow-down is there to suppliers' sub-contractors? Are they required to agree statements to the public which may affect your organisation and/or company valuation or reputation with you? Are there step-in rights in the event that a key supplier is unable to deliver? What are the liability limits if there is a catastrophic event? Do they have insurance? Are the overall clauses relating to cyber resilience adequate or is there a need to seek to renegotiate these? If the output of your supply chain reviews requires any renegotiation, prioritise the key contracts and areas of risk.
5. **Looking at the longer-term uplift**

- **Review board reporting and governance approach for cyber risks and security**: ensure that it is regular and meaningful to allow for appropriate oversight and challenge. Cyber governance increasingly involves a named executive owner and a cross-functional steering group.
- **Use ongoing and/or refresh staff training** to reduce the risk of successful phishing and social engineering attacks. Ensure that your team is trained up on the latest risks and types of attack.
- **Consider how you want to manage supply chain risk going forward**: review contract templates for cyber controls, audit and information rights, liability positions calibrated to exposure, cooperation in the event of incidents, sub-contractor flow-down and alignment with your own legal requirements. Review your supplier assessment and onboarding process to reflect evolving cybersecurity risks, including ensuring ongoing supplier risk reviews (not a 'set and forget' approach).
- **Consider what experts to have in place in the event of a cyber breach:** including whether you wish to have an agreed ransomware negotiator in place. The laws in some countries do not permit, or will not permit, ransomware payments, so consider your organisation's position in this area. Other experts include PR teams, forensic IT experts and legal counsel.
- **Check insurances**: if you have cyber-specific insurance, check the exemptions and ensure that there is liquidity in the business to deal with risk exposure. If relying on business interruption insurance only, check for cyber and other exclusions and ensure that the terms regarding non-physical damage / cyber are sufficiently broad. Look at what steps many need to be taken in advance to maximise the ability to instruct lawyers and specialists (such as forensic IT providers) of your choice promptly in the event of a cyber incident.
- **Regularly monitor changes in cybersecurity vendor offerings as well as evolving laws**, standards and regulatory guidelines to keep pace with requirements and best practices.

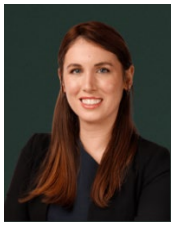
Now is the time to engage

Organisations affected by cyber incidents face multiple risks, including operational disruption and business interruption losses, exposure of confidential and sensitive information, reputational harm and loss of client trust, as well as the potential for regulatory sanctions and follow-on private claims and disputes. AI is accelerating both cyber-defence and cyber-attack capability, compressing timelines and raising expectations of preparedness. Future models are likely to be more capable still. Cybersecurity must be faster, make good – and safe – use of technologies in checking vulnerabilities and testing defences, and be more tightly governed, with clear contractual, operational and regulatory alignment. There is a risk of a growing gap between organisations able to keep pace with AI-enabled threats and those left increasingly exposed. Now is the time to strengthen core security measures, response readiness and supply-chain controls.

Authors

Jonathan Kewley
Partner and Co-Chair of the Global Tech Group, London

jonathan.kewley@cliffordchance.com
+44 207006 3629



Rita Flakoll
Global Head of Tech Group Knowledge, London

rita.flakoll@cliffordchance.com
+44 207006 1826

Other contacts

Stella Cramer
Partner, Singapore

stella.cramer@cliffordchance.com
+65 6410 2208

Caroline Dawson
Partner, London

caroline.dawson@cliffordchance.com
+44 207006 4355

Megan Gordon
Partner, Washington DC

megan.gordon@cliffordchance.com
+1 202 912 5021

Alexander Kennedy
Knowledge Director – CE Tech Group, Paris

alexander.kennedy@cliffordchance.com
+33 1 4405 5184

Holger Lutz
Partner, Frankfurt

holger.lutz@cliffordchance.com
+49 69 7199 1670

Patrice Navarro
Partner, Paris

patrice.navarro@cliffordchance.com
+33 1 4405 5371

Gunnar Sachs
Partner, Düsseldorf

gunnar.sachs@cliffordchance.com
+49 211 4355 5460

Dessislava Savova
Partner, Head of Continental Europe Tech Group, Paris

dessislava.savova@cliffordchance.com
+33 1 4405 5483

Herbert Swaniker
Partner, London

herbert.swaniker@cliffordchance.com
+44 207006 6215

Samantha Ward
Partner, London

samantha.ward@cliffordchance.com
+44 207006 8546

Charlotte Walker-Osborn
Knowledge Director –
Tech Group (UK Lead), London

charlotte.walker-osborn@cliffordchance.com
+44 207006 2662

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ