

Data breaches and deep fakes

Is your house in
order for 2024?

The latest wave of cyber-attacks, increasingly high-profile data breaches and the widespread adoption of artificial intelligence is changing the workplace and opening new reputational risks.

2023 has been a year of huge advances in AI and 2024 is set to be even more transformational with the rollout of technology such as Microsoft's Co-Pilot and the long-anticipated integration of generative AI into Apple's iOS.

The pace of technological change has led to the democratisation of content creation – from computer code to digital art, audio and video, what were once specialist skills have opened up to millions, who can now create plausible (if not always original or distinctive) digital assets with nothing more than a text prompt. Hacking and phishing techniques, which were previously the preserve of skilled criminals, are now in the hands of less sophisticated groups putting your organisation's data – and your reputation – at greater risk than ever.



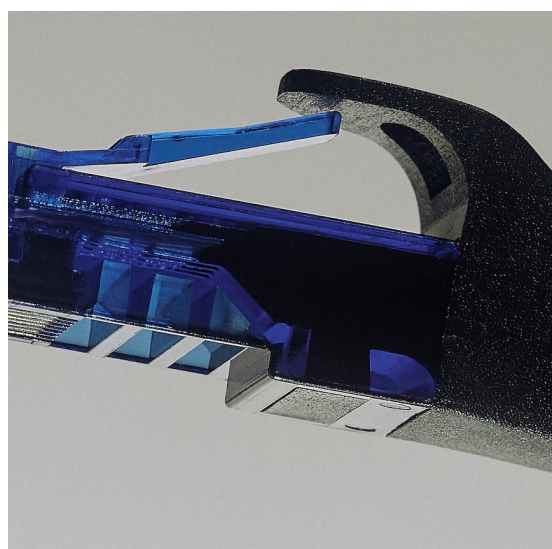
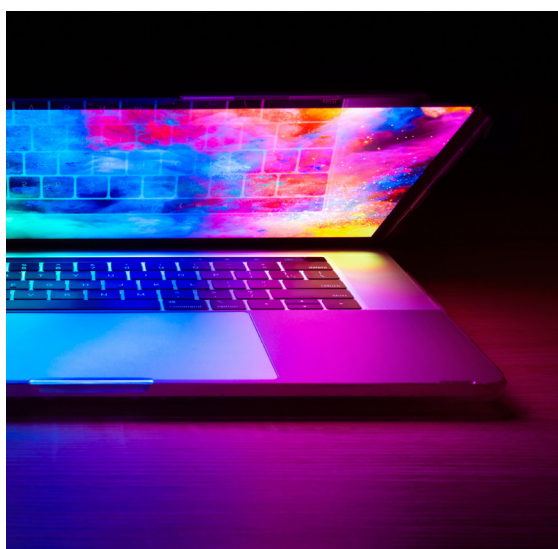
At this pace of change it is difficult for organisations to keep up with the reputational risks that arise as a result of (or are enhanced by) the rise of AI. Some of these risks are:

Cyber breaches disrupting business continuity and leading to negative media coverage and social media storms;

A well-meaning member of staff using an AI chatbot to 'tidy up' the language in your investment strategy or results announcement leading to this information being used to train the AI model for future answers – a potential compliance breach;

A journalist, under huge pressure to delivery more stories with fewer resources than ever, referencing something incorrect about your business as a result of an AI 'hallucination';

A malicious actor attempting to move your share price by creating and releasing a deepfake video of your CEO.



Questions every management team should be considering:

Is our crisis handbook/protocol fit for purpose and ready to deal with these new threats?

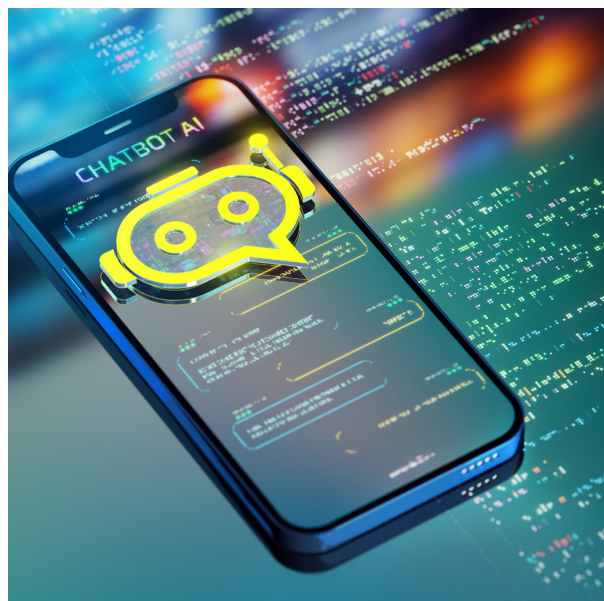
What AI usage policies do we have in place to prevent staff from inadvertently leaking confidential information?

Do we have a plan to react quickly to prove that potentially damaging information is false or a video is fake?







Do we know what has already been generated about our company and senior executives by AI tools?



Whether you already have a comprehensive crisis plan that requires stress-testing for regulatory compliance or you are concerned that your organisation is under-prepared for this new AI world, SEC Newgate is here to help in the UK and internationally.



Some of the services we can offer:

- 
 Ultra-realistic crisis scenarios using our simulation platform to emulate your real-world working environment;
- 
 Crisis handbook creation/updates to reflect the risk environment of the 21st century to ensure regulatory compliance;
- 
 SEC Newgate crisis app, developed by our crisis experts and technology partners covers everything you need in a crisis situation;
- 
 Online profile audits examining what AI chatbots are saying about you and your business, with recommendations on online clean-up work to minimise the risk of hallucination and misinformation/disinformation;
- 
 AI awareness training for your staff at all levels to minimise the risk of data leakage;
- 
 Support with writing AI usage policies and protocols for staff and other stakeholders.

For more information about any of these services or to speak to one of our reputation management and digital specialists, please contact:

ai@secnewgate.co.uk or urgent@secnewgate.co.uk