TECH MONITOR

IN PARTNERSHIP WITH

HEXAWARE

Thriving in the Age of Generative AI:

Harnessing possibilities to maximise business value

Senior leaders from a cross-section of industries met at The Mercer, in London, for an exclusive dinner and roundtable, held in partnership with Hexaware. The event was hosted by *Tech Monitor*'s features editor Greg Noone, who led a discussion, held under Chatham House Rules, around maximising business value with generative AI.

Introduction

While the origins of AI and its possibilities date back to the 1950s-60s, 2023 saw it truly hit enterprise maturity, spurring conversations across industries and prompting more digital transformation to facilitate generative AI models. This boom in generative AI capabilities stems from increased data availability, advances in computing power and new algorithms, unlocking ways to produce original content with more accuracy and realism than ever before.

However, some businesses have been quick to adopt generative AI and use it prolifically, while others have yet to leverage its potential. From distrust to cybersecurity, senior leaders are poised to interrogate and analyse the potential of generative AI for their businesses to increase efficiency and productivity while saving costs.

Tech Monitor's features editor Greg Noone invited senior leaders from various industries to share their views on the capabilities of generative AI to maximise business value, discussing levels of trust, the need for cybersecurity, data protection and risk management, as businesses look to find new ways that generative AI can optimise their business successfully.

Putting generative AI to use

How are businesses utilising generative AI to improve workflows and enhance operational efficiency?

Most speakers overall were cautious to rely too heavily on generative AI, due to a lack of trust in the chat-based solutions opened up for public use (e.g. ChatGPT). One CISO at a legal management firm, on discussing the prevalence of generative AI technologies, acknowledged how many staff were discovered to be using it at their business. "And, on Valentine's Day this year, we blocked it," they said. This allowed them to set guardrails for the use of generative AI technologies to be re-introduced more safely. "We set up a central AI accelerator function to look at the security, the risk, the compliance and legal implications," said the CISO. The firm is now an enthusiastic user of Bing Chat Enterprise and is "very pleased to be on the M365 Early Adopters Program," which is guided by Microsoft's Responsible AI Standards and Principles.

As delegates discussed the most effective use cases of implementing generative AI, document organisation and processing, meeting summaries and streamlining workflows were among the top suggestions. The CISO, who emphasised a cautious approach when utilising generative AI, also highlighted how the software has been able to carry out tasks far more quickly than manual labour would permit: "We produced 20 security awareness articles in a day. It would normally have taken us a day each".

The greatest challenge however, emphasised the speaker, is determining which of the multitudes of use cases for generative AI should be prioritised. "It's identifying those which are easy to do and high value," they said. "There aren't that many

"It's getting the balance right. As with any new technology, if you're too cautious about it, you lose market share, you lose ground."

– a CISO at a legal management firm

areas where we are saying 'No.' So, we currently still say, 'No PII must ever go near an AI.' But, I think all those things will soften over the next month or so."

Another security lead at a major retail bank discussed the use cases of generative AI their enterprise has been investigating, from written content to making security teams more efficient, particularly around incident response, where being able to quickly find the relevant terminology to a case they are investigating would be a key area of focus to realise efficiencies. "We've also looked at use cases around monitoring adverse media coverage. We've got a large retail presence in the UK," they said. "We get a lot of inbound communication from social media channels and something like a generative model... can look at the sentiment analysis for that communication, it's hugely, hugely valuable."

Trusting generative AI

What are the limitations of generative AI and why must we tread carefully?

One insurance executive highlighted the need for hypervigilance about whether to trust generative AI outcomes and the awareness and responsibility needed of those using open-source AI models in auditing, acknowledging that key stakeholders and staff are employed for specific roles to be fulfilled rather than the software itself.

When discussing the likelihood of hallucinations, an IT department head at a major bank highlighted how, without a preliminary understanding of generative AI, it is difficult to acknowledge and understand the nuances in production that such models can create.

When the speaker prompted the model to write a report of a tool demo, the generative AI tool gave mention to a web security analysis tool in the methodology that had not been used, thus giving false information about the process in the report. "Putting that to a stakeholder, they might well question that. They might be oblivious, but it would then reduce the validity of the report, so you still need that human expert to review what it is that the model has produced."

"Even if you are prepared to do lots of prompt engineering work to try to reduce hallucinations, they can, and will still happen. That's the nature of the tool – they're probabilistic, not deterministic."

– A security architect from a major bank

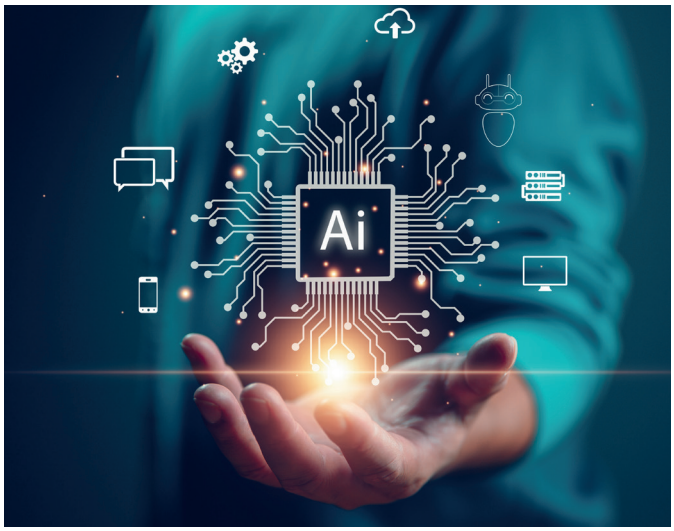
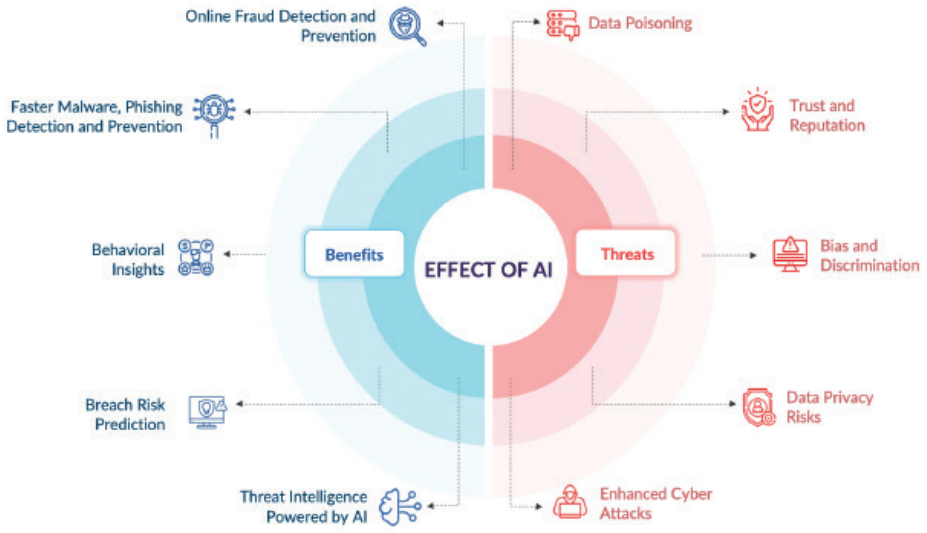


Figure1: Bright and dark side of AI in Cybersecurity

Generative AI tools have infinite possibilities to unlock new capabilities in improving cybersecurity, but we must also understand the threats that AI poses.



Safeguarding businesses

What are the cyber-attack scenarios associated with generative AI and how might these evolve in the future?

When discussing the potential of generative AI usage in cybersecurity, the legal firm security lead said that tool vendors of email gateways and DLP (data loss prevention) solutions say they are embedding AI into their solutions, but some are referring more to machine learning. "We get an awful lot of reports on DLP alerts, and 95% of them are false positives," the speaker said. "It's about finding that 5%."

The speaker highlighted how cybersecurity threats can be realised by testing the profiling abilities of generative AI tools to assess what information can be surfaced about individuals. Security teams can then navigate how phishing emails can become more targeted with tailored information using individuals' personal information. More airtight cybersecurity solutions can therefore be developed in response to more closely being able to identify these threats.

> **"User base analytics is always going to grow; the more you understand how your users behave, the better protected you can be when it comes to user behaviour-based attacks."**
>
> **A CEO from a skills development platform**

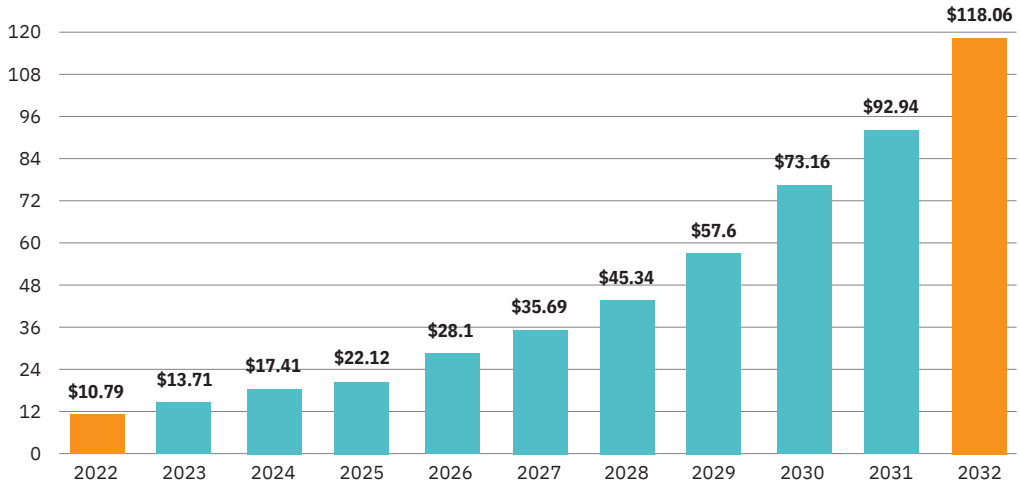
One global bank CEO said that they receive such phishing emails on a daily basis. "Somebody hacks the email ID, then generates - and the whole big email comes along, the same style as what you would have written," says the speaker. "Then, when our people call up the number, it gets diverted and the AI 'robot' speaks in the same manner that you would speak." This highlights the increased sophistication of AI tools and capabilities that will become an increasing cybersecurity risk, not only to banking, but all industries managing sensitive data.

One delegate mentioned a scenario considered around deepfakes, where a believable video of a senior leader goes online before the markets open to announce a divestiture, resulting in someone shorting the market, proposing the question of what to do in response. One speaker responded with the suggestion that deepfakes could be more widely detected with processes whereby secondary information is checked against this content, such as press releases surrounding any significant announcements. The difficulty here, however, is the turnaround time needed to determine what is a deepfake, which can have serious wide-reaching financial consequences, even if reaction takes only up to one hour. The slower the response, the greater the risk of cost a business can lose.

Figure 2: Generative AI market size, 2023 to 2032

(USD Billion)

The global generative AI market size was evaluated at $10.79 billion in 2022 and is expected to hit around $118.06 billion by 2032



Source: www.predenceresearch.com

What strategies are business leaders adopting to safeguard their businesses from cyber-attacks associated with generative AI?

Delegates highlighted the benefits of a variety of tools and platforms, including Github Copilot and CodeWhisperer, where the effort needed to utilise some over others becomes counterproductive. One positive of these tools was huge productivity improvements, helping junior to mid-level programmers. While high-level programmers are more experienced, these tools can function as a method to upskill and increase productivity and quality across different levels of roles.

Another delegate provided an example of an open-source threat modelling system they had built to help increase efficiency and free up time. "All it's doing is trying to put a mediocre security professional in the room and to generate a first-pass threat model for a given application script," the security lead says. The model is fed a natural language description of an application and it responds with a methodology. While it is not a finalised product, it provides security teams the chance to focus on more complex issues by freeing up time and increasing efficiency.

How can businesses ensure they are at the leading edge when using generative AI?

A key limitation with generative AI was brought to discussion by one security lead at a legal management firm who described how, when asking generative AI tools to search their intranet to find a policy, the tool surfaced an out-of-date policy as the company had not removed this from their intranet, prompting the need for the business to clean up their corporate data and ensure that data is up-to-date if they expect to use this to train models. "When we ask generative AI tools to surface our intranet and find me a policy on such-and-such, half the time it comes up with an out-of-date policy because we haven't done a clean-up," said the speaker. "That's going to be a humungous undertaking."

In response to the point of data quality and relevance, one delegate suggested that "bad data" is synonymous with data that is not 'current'. In some cases, if data is not up-to-date, decisions cannot be based on that data, particularly in tax rules and regulations, or legal cases or precedents that have been announced in Europe and how that differs to other territories, listed the speaker. Companies should therefore update the accuracy and efficiency of their data if they are to use generative AI properly which is a huge task.

Looking to the future

What is Hexaware's outlook on adoption of generative AI?

Hexaware is marching ahead with cautious optimism, in guiding its customers on generative AI adoption. The business is observing that organisations are still primarily in an evaluative mode. They are exploring the various technological solution paths out there, keen on identifying opportunities where they can clearly achieve measurable ROI while ensuring that there are no compromises from a data security and reliability perspective. Hexaware's Generative AI Consulting and Implementation Framework is designed to guide its customers on this journey across the entire lifecycle.

Research estimates that generative AI could add the equivalent of $2.6 trillion to $4.4 trillion in annual economic benefits across 63 use cases.

Source: McKinsey

Generative AI is a rapidly evolving field that has the potential to transform various aspects of business, science, and society.

What should businesses consider among discussions on generative AI?

- Generative AI has the potential to revolutionise businesses by driving innovation, boosting operational efficiency, and customising experiences.
- It can generate diverse content, automate tasks, and personalise interactions, catering specifically to targeted audiences through features like chatbots and precision advertising.
- Generative AI can also help businesses with improving decision-making by providing data-driven insights, enabling businesses to optimise strategies and operations with informed perspectives.
- However, generative AI presents challenges for businesses, including issues like inaccurate content, ethical dilemmas, and societal impacts.
- These challenges involve data quality, ethics, legal risks, and potential displacement of human workers.
- To navigate these issues, businesses should adopt responsible AI practices, ensuring data quality, promoting transparency, and engaging with stakeholders and regulators.