Hey! What's New? 2024-107

Becoming Guardians of Digital Trust

According to a *McKinsey Digital* article, Generative AI has increased the focus on data, putting pressure on companies to make substantive shifts to build a truly data-based organization. "The excitement around generative AI (gen AI) and its massive potential value has energized organizations to rethink their approaches to business itself. Organizations are looking to seize a range of opportunities, from creating new medicines to enabling intelligent agents that run entire processes to increasing productivity for all workers. A raft of new risks and considerations, of course, go hand in hand with these developments. At the center of it all is data. Without access to good and relevant data, this new world of possibilities and value will remain out of reach."

As risk has become much more of an area of concern with the rise of advanced technologies, governments are moving quickly to roll out new regulations, and companies are evaluating new policies.

Some of the issues have been well known, the article points out, such as hallucinations (that is, gen AI models providing inaccurate answers), bias, intellectual property rights and data privacy. But, since these technologies are so new and evolving quickly, the broader risk landscape is often not well understood. According to the article, three types of risk stand out:

- *New types of attacks.* The power of gen AI to learn and evolve quickly is opening the door to completely new types of attacks, including self-evolving malware that learns internal systems and evolves to breach defenses, intelligent bots that can increasingly mimic humans, and infected data that is inserted into models training.
- *Broadening landscape for risk.* The broad interconnections between AI and data systems – both within and outside of enterprises – have created a significantly greater area for damage to be done.
- *New unknowns.* As interacting with AI becomes more conversational and less about just searching for facts, companies will enter a much more ambiguous zone defined by varying value systems. And with the proliferation of gen AI agents essentially "talking" with each other, completely new categories of risk will likely emerge.

To deal with these new risks, the article suggests several essential actions for data leaders. "In addition to keeping abreast of these emerging risk types, data leaders will need to rethink their approaches to risk. Many still rely too much on traditional data quality and compliance approaches, while few have started to implement advanced coding and ethics testing. This reevaluation should be underpinned with the understanding that risk management is a competitive advantage, achieved either by building a brand that is a safe custodian of customer livelihoods or by simply avoiding the failures that competitors might face. That view should drive a more proactive posture to addressing risks than simply hitting compliance benchmarks."

The article adds that data leaders (and tech leaders more broadly) can keep up with the scale of cyber issues by implementing AI (and eventually quantum) capabilities, such as "adversarial"

LLMs to test LLM-generated emails for inappropriate or illegal content, and fairness tool kits to test for bias.

But, it warns, “while tools developed by third parties can be helpful, advanced AI security shouldn’t be farmed out. Data leaders need to be mindful about building up their own capabilities to keep up with the pace of the market.”

As technology permeates businesses and society, the importance of data will continue to increase – as will the accompanying challenges. This section of the article concludes that “the levels of uncertainty and the rapidly changing dynamics of technology mean that there are few clear answers today. But, by sticking to the most important priorities and understanding the essence of the issues facing them, data leaders can navigate a path to a data-driven enterprise.”

For much more advice on how to become data savvy, go to Charting a path to the data- and AI-driven enterprise of 2030 | McKinsey.