THE SANTA FE GROUP

RISK REPORT

"Artificial Intelligence is going to change the world more than anything in the history of mankind. More than electricity."
— **Dr. Kai-Fu Lee,** AI Oracle, 2018

February 16, 2021

ARTIFICIAL INTELLIGENCE – THE RISKS, OPPORTUNITIES, AND WHAT BOARD MEMBERS NEED TO KNOW

By Charlie Miller

Most boards are just beginning to understand the extent to which the increased use of machine learning (ML) and artificial intelligence (AI) (see definition in Resources below) will test help to identify new market opportunities, speed product development, and increase competitive advantage. Every industry will be impacted: financial services firms, transportation companies, manufacturing firms, healthcare organizations, education at every level, media companies, and more. AI will transform your organization's policies, risk management oversight, operations, supply chains, and workforce.

Successful adoption of AI requires strong organizational oversight and leadership. Especially in the current COVID environment with fundamental changes to where, and the way, work is being done, boards have a heightened responsibility to ensure their organizations are equipped to handle the important AI challenges we've seen emerge. AI has become so important that the U.S. National Artificial Intelligence Initiative Office has been established to oversee AI research and policymaking across the government, private sector, academia, and other stakeholders.

This Risk Report focuses on three areas: big data versus privacy; AI models and bias; and workforce education and expertise.

BIG DATA VERSUS PRIVACY

Nowhere else is the potential tradeoff between big data and privacy more obvious than in the quest to feed artificial intelligence applications with ever greater amounts of precisely honed data. As processing power increases, the ability to harness data from an increasing array of sources in support of more sophisticated AI, applications have grown exponentially. Much of this data may be unencrypted. At the same time, increased regulatory scrutiny and updated privacy regulations such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act are still evolving relative to AI technologies and modeling solutions.

The new Administration will likely resume scheduling hearings focused on surveillance, counter terrorism, and social media AI algorithms. These hearings may well extend to include an examination of appropriate board responsibilities relative to oversight and governance of new innovative technologies, including: artificial intelligence, cloud computing, and digital transformation of risk management processes. Globally, privacy regulations already mandate organizations to obtain specific permission from consumers when utilizing their customer data for precisely defined purposes. Over time, privacy regulations in the US can be expected to follow suit.

Convergence of these two trends has created something of a high wire act, and boards must be cognizant of the implications of failing the balance test. Mature data governance regimes, which boards should ensure are in place, are key to navigating the increasing need for properly procured, properly secured and properly utilized AI solutions.

Questions boards should consider:

- Are AI applications in your organization being developed internally or externally?
- If AI applications are being developed (and perhaps executed) externally, does your organization have appropriate insight into how data feeding those applications is procured, secured and verified for appropriate use in the application?
- Does your organization have mature data governance policies and the ability to ensure compliance?
- How will your AI solutions protect your customers' privacy and ensure against the misuse of their personal and confidential information?

AI MODELS AND BIAS

Organizations must have a defined process and staff adequate to thoroughly test AI applications whether developed in-house or purchased from a third party. Testing oversight by experienced staff is critical.

Bias in AI is a well known issue. No matter how an AI application is used, deploying an AI application developed by a third party does not relieve your organization of the responsibility for ensuring the model's performance and understanding the basis for its output.

As AI models have become more complex, it has become far more common for developers to refuse to reveal the "secret sauce" that makes their applications perform. Often, this situation puts purchasers in a bind – and financial services regulators have begun to address the issue. For example, updated March 2020 OCC Guidance made it clear that, when purchasing risk management models, all Financial Institutions should: "…conduct a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities are sufficient."

A robust testing capability by both the developer and the purchaser is the price of entry for deploying any AI application in a corporate environment. And boards have an important obligation to make sure that such testing capacity is in place and routinely utilized. Every AI model and data set is subject to bias, even if that bias is unintentional. Bias can be introduced by the teams developing AI algorithms, teams selecting, prototyping and determining the data to be used with specific AI models, and even teams validating and interpreting the output from AI applications.

Questions boards should consider:

- Does your organization have a robust process for testing the accuracy of AI applications and the suitability of data that feeds them?
- Does your organization have a system of checks and safeguards to identify and learn from instances where AI applications fail to perform as expected?
- Does your AI team consist of multi-generational diverse individuals to further drive innovation and minimize unintentional bias?
- Does your organization have an incident response plan in the event an AI solution damages your brand?

WORKFORCE EDUCATION AND EXPERTISE

The impact of AI on our national workforce will increase at a rapid pace. McKinsey & Company research suggests that through 2030, the time spent using advanced technological skills will increase by 50 percent in the United States and by 41 percent in Europe. Dr. Kai-Fu Lee, a recognized AI expert and author, estimates that AI will displace 40 percent of world's jobs in as little as 15 years.

The need for increased skills in the areas of cybersecurity, data analytics, machine learning and artificial intelligence is already leading to a race to find scarce qualified resources. For example, manufacturing companies acceleration of digital transformation initiatives to achieve Industry 4.0 expectations complicates the expertise shortage issue. It is essential that top executives and governing boards understand how artificial intelligence will alter the size and nature of their workforce in the years ahead. An effective strategy for acquiring, upskilling, educating or partnering to ensure the timely availability of these must-have resources is essential to meet the AI-centric operational environment upon which your organization will increasingly rely.

Questions boards should consider:

- Does your organization have employees with proper skills to develop and successfully implement AI applications?
- Do your risk teams have the resources required to remediate AI enhanced threats?
- Do you have a plan for providing appropriate educational opportunities to prepare your employees for the coming AI-induced changes to their jobs?
- Do you understand the range of skill sets required for your organization to optimize the use of artificial intelligence applications?
- Have you considered AI's impact on your organization's workforce moral given the potential for job elimination?

RESOURCES

The Future of Artificial Intelligence

GDPR Article 22(1) - Rights related to automated decision making including profiling

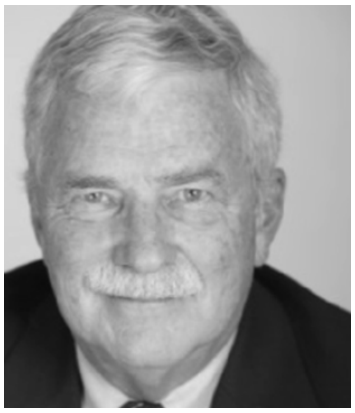
Surveillance Capitalism

Skill Shift: Automation and the Future of the Workforce

The Fourth Industrial Revolution: At the Intersection of Readiness and Responsibility

Artificial Intelligence (AI): The ability of machines to behave in a way we would consider "smart." The capability of a machine to imitate intelligent human behavior. AI is the ability to be abstract, creative, deductive — to learn and apply learnings. E.g., model risk development and fraud monitoring systems. Also see black box, machine learning, and deep learning.

ABOUT THE AUTHOR



Charlie Miller is a frequent speaker and a recognized expert in Third Party Risk. His key responsibilities include expanding the Shared Assessments Third Party Risk Management membership driven program, facilitating thought leadership, industry vertical strategy groups, continuous monitoring / operational technology working groups and IoT and Artificial Intelligence research studies. He joined The Santa Fe Group, Shared Assessments in 2015 and has been in the third party risk space for over 20 years. He has vast industry experience, having set up and led third party risk management and financial services initiatives for several global companies. As a consulting Partner at Deloitte, he led a financial services practice unit, focusing on technology outsourcing, risk management and cost control. He began his career at IBM as a systems engineer. Charlie is a Distinguished Fellow of the Ponemon Institute, Certified International Privacy Professional and Certified Third Party Risk Professional.

WHO WE ARE

The Santa Fe Group manages the Shared Assessments Program which, with more than 300 corporate members, is the industry leader in third party risk management guidance.

The Board Risk Committee (BRC) is under formation and will be the first non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC will be a trusted place for the exchange of ideas, best practices, and topics of interest.

CONNECT WITH US