WHAT SHOULD A BOARD UNDERSTAND ABOUT AI?

DR. EDWARD AMOROSO

The governing role of the board member is generally well-defined, but often misinterpreted by observers. So let me start with a reminder of what corporate board members are expected to do. First, they must participate in reviewing and overseeing management. This requires the skill to know when and where to chime in, and this is easier said than done.

Second, they must participate in corporate strategy to help drive the company to an optimal decision when something truly consequential is being considered. Major mergers and acquisitions, for example, generally demand the attention of the board, but minor, day-to-day management decisions do not. Again, the principle sounds easy but sticking to it in practice is not..

Finally, corporate board members are expected to review and ensure the accuracy of important financial statements and other key data reported by the company. This does not imply using a fine-toothed comb to review every ledger item, but it does require active enough participation to ensure that public reporting is correct.

In addition to these responsibilities, board members frequently find themselves wading into new areas of concern that their companies confront. Cybersecurity is one such area that has spurred considerable debate about whether directors should play a significant role in making decisions, and if so, how involved they should be. Certainly, they are not expected to be security experts, but general agreement exists that broad awareness is now necessary.

A comparable issue involves artificial intelligence (AI). In recent months the public dialogue has been intense (to say the least). You can be sure there have been innumerable private conversations behind closed doors. What are AI's implications for the business? And by the way, how will it affect security? Just as corporate directors are not expected to be experts in that field, they are not expected to be experts in AI. But a consensus is emerging that it is a key aspect of a board's responsibilities.

That said, what are the key considerations for board members on this subject? What should they know about the business implications and security implications? How much do they need to understand about this important technology?

Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

BUSINESS IMPLICATIONS

The effects of AI on business will differ from one industrial sector to another, but some general statements can be made. Hopefully, these broad characteristics in the context of modern business will start the intellectual process for board members to begin integrating AI-related impacts to their governing responsibilities.

Below I've listed issues with an emphasis on how they relate to boards. I've skipped over those that might have a substantial impact on business but not on board responsibilities. Please keep this in mind. My guidance here is for boards, not day-to-day executives and practitioners.

Business Writing Will Become Software-Defined

Board members should recognize that for many years the quality of normal business writing has varied considerably. I'm talking about the memorandums, policy statements, agendas, meeting minutes, and other narratives that have been used in business for decades.

The problem is that so much of this writing has been just terrible, often including nonsensical reports, lengthy papers, and unclear narratives. Board members are certainly familiar, for example, with the large volume of often unintelligible materials presented in advance of meetings. This is common across all aspects of modern business.

AI will have a direct influence on the quality of these written artifacts because automation is so well-suited to this task. Auto-generated notes after online meetings are already common, and this will extend to a fully software-defined approach to business writing that will have considerable consequence on all forms of business communications. And it should represent a tremendous improvement.

AI Will Drive Business Macro Trend Analysis

Board members and corporate executives have depended for many years on the predictions and observations of trends in the marketplace. These often come from industry analysts who opine based on their admittedly limited view of the many factors that influence any type of prediction.

While there will always be interesting personalities who can provide incisive and even humorous observations on macro trends, the use of AI to analyze market trends will be a more common occurrence. The advantage AI has is that it can include virtually every factor for which some evidence is available to drive the optimal prediction.

Board members should expect to see a symbiotic relationship between human and automated market trend analysis. Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

> The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members.

Customers Will Learn to Accept AI for Certain Applications
The ongoing debate with respect to the suitability and acceptability of using AI for certain applications will gradually wane in favor of societal acceptance of the technology. This happens for every new technological advance, including early industrial advances as well as the advent of computing.

The implications for board members is that aggressive adoption of AI, where appropriate, is the best course of action, and hesitation related to concerns about societal qualms is not recommended. Certainly, regulation and some degree of control will be required, but I advise businesses to be aggressive.

SECURITY IMPLICATIONS

The security implications for any type of business will involve offensive considerations ("Can we be hacked by an adversary using AI?") as well as defensive considerations ("Can we use AI to protect ourselves from an adversary?"). As one would expect, use of AI for both is an obvious corollary.

Below I lay out key security-related issues that emerge for board consideration. These should be addressed and coordinated across the entire management chain, and that should include the chief information security officer (CISO).

Major Adversaries Will Use AI to Attack
An important recognition that every business must understand is that their country of origin will certainly be targeted by nation-state adversaries using AI-based offensive measures. Organizations located in the United States, for example, should expect that countries such as China and Russia will most likely develop and use these methods.

The implication from a corporate perspective is that the front line for cyber threats is not the military or even the government, but rather is the distributed collection of data from business, enterprise, industrial groups, families, individuals, and other non-government targets. This is where an adversary nation will target with cyber threats.

Countries Will Need AI to Protect Infrastructure

Special consideration is obviously needed in protecting critical infrastructure, if only because the consequences of an attack can be so much more severe than attacks to other sectors. For board members with responsibility to manage critical and essential services, the need to maintain secure defenses against AI-based smart attacks will be paramount.

An implication of the existence of AI-based offensive cyber methods is that organizations will need AI-based defensive measures to put a reasonable protection in place. It should be obvious that if an automated attack is being levied, then the defender will not be able to stop such an attack merely by using manual, procedural methods.

Board members should be cognizant of major investments in AI-based security infrastructure, not to review or approve the specifics of the technology or vendors selected, but rather to ensure that a strategic plan is in place to maintain the ability to stop these new forms of attack with a solid AI-based protection scheme.

Social Engineering Will Benefit from AI

One attack that all board members will be familiar with involves the use of social engineering tactics to trick an individual into sharing sensitive information or to perform inappropriate tasks such as transferring money from one account to another (e.g., through fake text or email to a finance officer).

The foundational basis for social engineering involves skill to take advantage of the trust of a targeted person, and this requires having information about that target. Since AI is so good at collecting and analyzing information to establish context, it should be expected that social engineering, including phishing, will become more difficult to stop.

As with nation-state attacks, social engineering attacks will also demand a strategic plan to ensure proper protection. Boards should monitor their companies' defensive programs and should request to see evidence that these are working. Past methods, such as phish testing, will be useful components but will not be sufficient as the basis for such protection plans.

BOARD OBLIGATIONS

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members. I wrote this article with this initial goal in mind.

In addition, however, there are emerging tasks that should become part of the day-to-day board ecosystem. While these tasks will evolve over time, let me point out a few below that I expect to see become important in the coming years. Local business conditions should certainly be used to tailor these general points.

Mergers and Acquisitions Must Include AI as a Factor

If the organization regularly performs mergers and acquisitions (M&A), then it must become a standard component of the evaluation rubric that potential AI disruption be considered. The last thing any organization needs is to make a major investment in a company that will soon be disrupted or even replaced by AI.

The M&A team should be directed by senior leadership, with governance from the board, to ensure that this factor is thoroughly considered, especially for mergers that are sizable with consequence to the firm. Without such careful scrutiny, the possibility of a poorly conceived merger or acquisition seems possible—and potentially disastrous.

Human Decision-Making Will Not Be Replaced by AI

A commonly stated point in the popular media, and one that might have some influence on board member thinking, is the claim that AI will replace human decision-making. This may be true in certain situations where data is perused and processed in a structured manner. Radiologists, for example, might replace certain of their data tasks with AI.

The suggestion, however, that this will occur in the context of board strategy, corporate governance, and organization oversight is not reasonable. Good board governance will make use of technologies such as AI to ensure optimal context for discussion and debate, but robots are not likely to gain a seat at the board any time soon.

Cost Reductions Can be Considerable Using AI

One advantage that AI does bring to most business contexts is the ability to reduce cost. Customer care, help desk support, and other tasks that involve procedural steps will be good targets for such reduction. And boards would be wise to establish oversight where such cases are being considered.

The goal, obviously, should be to balance the needs of the firm for cost optimization with the needs of customers, who will demand high quality interactions, and also the needs of employees to feel safe that their career paths will be preserved—or at least guided toward areas that will complement the use of advanced technologies such as AI.

ACTION PLAN

The best course of action for corporate boards and individual board members may have already begun with perusal of this article. Education will be a key differentiator between boards, and any governance team that takes the time to learn the implications of AI will have a clear advantage.

My advice for an action plan is to over-index on education and training. The steps implied by the comments above should be included in local planning, but each organization is different. In the coming years, board members will have to earn their paychecks by developing effective plans for governance and oversight in this new technological era.