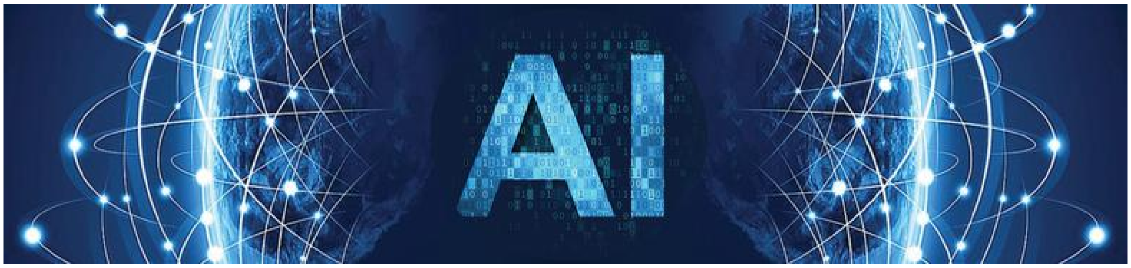
Legal BlackBook™

Home
Editor's Note
Cozy with the FBI
Legal's Role in AI Strategy
GDPR for the U.S.A.
Cyber Reading
Cyber in the News
The Year Ahead
Building Bridges
Public-Private Clash
What the Numbers Say
About Us
Archive
Subscribe for Free
Privacy Policy

CyberInsecurity

April 2018

INTERVIEW: ANDREA BONIME-BLANC / GEC RISK ADVISORY



THE LEGAL PERSPECTIVE HELPS SHAPE AI STRATEGY

Companies need multidisciplinary teams to find the right path.

Andrea Bonime-Blanc has a new book called The Artificial Intelligence Imperative: A Practical Roadmap for Business, which will be published by Praeger in April, and the timing couldn't be better. AI seems to be everywhere these days, and Bonime-Blanc can talk about it as a business consultant, an expert on corporate governance and a former general counsel. She is the founder and CEO of GEC Risk Advisory, which specializes in governance, risk, ethics and compliance. She worked for two decades as a C-Suite executive. In addition to her stints as a general counsel, she has served as a chief risk officer, ethics officer and compliance officer, among other positions. All of those perspectives come into play when she talks about the risks and rewards of AI. The interview has been edited for style and length.

Andrea Bonime-Blanc

Legal BlackBook: *You've talked about the need for "traditional" companies to focus on artificial intelligence. What do you mean by "traditional companies," and why have you particularly addressed them?*
Andrea Bonime-Blanc: One of the areas that my co-author [Anastassia Lauterbach] and I were concerned about is that you have, on the one hand, the leading technology companies—Apple, Facebook, Amazon, Google and Microsoft. And there are other big players like IBM and more niche technology companies that are also very attuned to AI. But then you have a vast world of businesses where some people are dipping their toe into AI. They don't really know what to do. And you have a fourth group, which is the old-line industries that haven't figured out what these new technologies really mean to them: the chemical industry, oil and gas, manufacturing. Some are doing the right thing and starting to inquire. But many are not. Many don't think it's important and don't think it's going to affect their businesses. We want that large group to start thinking about AI as important, because sooner or later, through data analytics or other forms of information gathering and application of AI algorithms, some of these industries that are very traditional may get disrupted. Look at cases of past companies that missed the technological change that was impacting them. Kodak invented digital photography, and they didn't pursue it, and someone else ate their lunch. So don't let this new technology pass you by, put you at a competitive disadvantage or disrupt you out of existence. That's the attitude that we have in the book.

LBB: *You've talked about the risks and rewards that AI offers. And you've presented different kinds. Let's start with cyberattacks. What are the risks that AI poses there?*
ABB: AI is going to be used as a tool by people who are savvy about cyber. If you have sophisticated AI algorithms in the wrong hands, that would be a risk. For example, if the bad guys—nation states, criminal gangs, the fat guy on the bed—want to use AI as part of their cyber weapons, that's where the serious risk occurs.

LBB: *What are potential rewards?*
ABB: The counter to that is that the military, cyber experts and governments are also developing AI tools to use in cyber warfare and cyber defense. AI can become part of the mutually assured destruction that we had with nuclear weapons. And when used by the people who are defending the integrity of business assets or government assets, it can be something very beneficial. It will help you find out about attacks while they're happening. So it can be both a tool for good and a tool for bad.

Companies that ignore AI may find themselves disrupted out of business.

LBB: *You also talked about the ethics and governance challenges that AI imposes. What are some key issues there?*
ABB: From an ethics standpoint, what we're most concerned about is some of the issues that come up with how AI is created in the first place. And it always goes back to the humans involved. Most programmers are young, well-educated men. If you have a bunch of young white males who are well-to-do creating the algorithms, you're missing out on a very large swath of society. You may be missing the perspective and the wisdom and the knowledge that women might have and that older people might have, that people from other geographies might have. So the diversity piece is an important ethical issue. And who has access to AI is another issue that has societal implications. Who is using AI, who can use AI—there are some inequality issues. Also, there's the employment and labor impact. How many jobs won't exist tomorrow as a result of AI and robotics? I was just in the Midwest yesterday visiting with a client that's in the energy sector, and one of the questions they have is, How will AI and robotics impact their labor force? They have a lot of blue-collar workers doing manual work. As robots and AI become more

sophisticated, these jobs are going to disappear. What is the responsibility of a business in planning for that, maybe retraining the workforce? There's also a good news story buried in there. When there's major technological disruption in the marketplace, a lot of new jobs that nobody foresaw also emerge. Some of the new jobs that are being talked about are AI data designers, AI data trainers, people who help to decide what data goes into the algorithm.

LBB: *A central point you make is that the way a company handles AI can have an impact on its reputation.*
ABB: Take the Equifax situation or Anthem, where privacy data was hacked or stolen and ended up on the dark web. So companies like Anthem and Equifax that have this treasure trove of privacy data, if the AI algorithms they use to understand and develop and manage the data and then to interact with customers are not going through very clear and systematic quality management, they may actually expose themselves to cyberhacking. And that can be a huge reputational risk.

LBB: *We hear all the time about reputations being damaged from cyberattacks. How can a company mitigate the damage?*
ABB: I did a research report for The Conference Board on cyber risk governance, and we looked at several cases, including Anthem, Target, Sony and J.P. Morgan Chase. Each of them was attacked and hacked in different ways, but I looked at the reputational risk profile for the four entities, and they were very different cases. And if you take the J.P. Morgan case, where they were already spending a good $250 million a year on cybersecurity, their reputational hit was lower than, say, an Anthem or Target, who apparently didn't have very strong defenses, and it was clear that they had not paid as much attention as J.P. Morgan had. I had statistics on that in the report using data from a Swiss company, RepRisk, that creates a reputational risk index on companies based on media and social media responses. The idea there is that if you build the resilience—that is, you know what your risks are, and you've actually created the right kinds of programs, training and controls to try to mitigate that risk, and then something actually happens—the market and the stakeholders are going to be a lot more forgiving than if you never do anything or you do it negligently, which certainly came out in cases like Target, Anthem and, more recently, Equifax.

LBB: *You've been a general counsel yourself. What role should the GC play in creating and managing a company's AI strategy?*
ABB: The most important thing to do as a general counsel is, first of all, to inform yourself of what AI means and how it might affect your particular business. So do some investigating on your own. But in terms of the responsibility to the company and the shareholders, a general counsel can be a very important player—a key player, actually—in helping to structure the right approach in the company, creating a cross-functional team. You want to have some key players looking at this issue in a very concerted way. Depending on the industry, this could be the general counsel along with other key members of executive management—operations, innovation, strategy, IT, risk management, R&D. Clearly, another important aspect of this is the executive team—making this part of their strategic review. Assuming that the general counsel is part of the executive management—I know that a few aren't, which is shocking to me—but it really has to start with the executive management. "What are we doing about AI?" Once the C-Suite has figured out what they need to do, then the general counsel can be part of an ad hoc committee that is looking at it more proactively. The GC, of course, is looking at the compliance, legal and regulatory issues that might be involved, but other people are looking at their areas and really sharing the information.

Then they can bring in experts to talk to them, do some further research. But it has to start at the C-Suite in terms of the strategy of the company. "Do we bring AI into the picture? Do we need to? Or are we going to be subverted and disrupted by a competitor that is using it? Or is there a completely different business model out there—an unforeseen disrupter—that is going to upend our business?" Look at Amazon with retail, right? They came out of nowhere, and they're disrupting Walmart. The point is: How are you going to incorporate this into your strategy? Who's going to look at it within the company? I think the GC should always be part of that group.

LBB: *You talked about the general counsel educating himself or herself. How much expertise in cybersecurity and artificial intelligence does a general counsel need?*
ABB: It depends on what kind of business and industry you're in. At a minimum, we should all be informed. We should all be curious, because it's affecting our day-to-day lives—both cyber issues and AI issues. We're using AI in our phones right now, and we don't even know that we're doing that. And we're being cyberattacked, and our personal information is being stolen by cyber criminals on a daily basis, so as a citizen I would say that we all need to be somewhat informed. As a general counsel, there's a heightened responsibility not only to be informed but to keep up with the legal, regulatory and compliance requirements that are coming down the pike for your industry. Clearly, it's part of the big bucket of technology affecting your business, as more and more technology is doing. We're at the threshold of a potential major technological disruption of the financial sector through blockchain and cryptocurrency. I don't know enough about that to give you advice, but I know that if those technologies achieve what they aim to achieve, they're going to completely disrupt the banking sector as it exists today and the way we pay for things —and the way we create transparency and accountability around those things. So depending on what industry you're in, the GC really has a responsibility to be personally informed, to be legally informed, and then to be informed in a way that they can be a contributor to the discussion at their business—at the executive level and, frankly, vis-à-vis the board as well.

LBB: *Speaking of which, let's turn to the board. A focus of your work has, for a long time, been the board of directors. So what should the board's role be?*
ABB: To take the 50,000-foot view, boards have an obligation to understand how AI and other technologies intersect with the business. Even if you're in the most traditional kind, you have a responsibility to understand if, from a strategic standpoint, your business is going to get disrupted. And/or, will your business achieve a competitive advantage if it starts incorporating some of these tools? So if I'm a director of a widget company and we have traditional factories around the world, I would be asking myself: "How do we use technology in our widget factories to enhance value for the shareholders?" And that might lead to a discussion of: Who is in the factory right now? What means of production are they using? Are there robotics involved? If there aren't, why not? Are our competitors ahead of us in thinking about how technology is incorporated into and improves the productivity of the company? Again, very big-picture, that's their responsibility.

But we're talking about governance. While the executive team has the responsibility to develop and implement the strategy, the board has oversight responsibilities. Both of them share responsibility for a number of steps toward understanding AI. There has to be discussion for the full board about data. What data do we have in our organization? What data value strategy do we have? Do we have information that could be deployed into an AI algorithm that could create efficiencies, create differentiation and new ways of understanding and delivering our products and services? And then you bring in outside experts to help you think about this. Obviously, you want to have people like your chief information security officer, chief technology officer, chief risk officer, general counsel—those people need to be part of that discussion.

The general counsel can be a key player in helping to devise an AI strategy and creating a cross-functional team to implement it.

A key additional point here, both at the C-Suite level and the board level, is that you want to have a very clear idea of your talent management. Who do you have managing technology information security? Do you have the right people? Do you need new people? And that has to be done in conjunction with the chief technology officer. And then you also need to have that futuristic look of understanding where this is going. How it will affect key stakeholders in the organization, especially employees and labor, but also third parties, customers, the media, the government, the regulators? Another thing that I think is really important with the board is that it needs to have a couple of people who can talk about this—understand what questions to ask. Even if they're not tech experts, they understand cyber. They understand technology. And they can ask the chief technology officer, the chief information security officer, the general counsel in some cases, the right questions about how they're managing data, and how it will interface with AI—and how AI will interface with the company's products and services.

LBB: *If a company doesn't have directors who match that description, should they be trying to give a couple of people intensive training? Or should they be out there looking for new directors to bring in, who already have at least a pretty good understanding of cybersecurity and artificial intelligence?*
ABB: Both options are good. Part of the challenge you have in governance and boards, and this goes beyond technology, is that you usually have similar, homogenous people. Not diverse. And by that I don't just mean gender and race. You have people who have been CEOs and CFOs. They're all sophisticated people and have done a lot in terms of their career, but their worldview is based on running businesses and financial matters. And this whole cyber development and these new technologies coming around—AI and blockchain and so on—are complicated and require some additional firepower on the board. You can train people, you can give them intensive courses. NACD, for example, has a cyber risk governance certificate for boards. And that will be helpful. But depending on the business you're in and how disrupted it might get, you really want to bring in some of that new blood that is conversant with and maybe even very knowledgeable about technology in general and the particular industry that the company is in. I'm also a big proponent of folks who, like me, have a legal background sitting on boards. Again, they bring a view that is a little different from the technical, financial and operations person. Also add chief risk officers—people who have done that kind of work—because they bring the risk lens into the picture, and with it a broader view.

LBB: *What percentage of the Fortune 500 would pass muster right now if their boards were examined to see if they had individuals with the kind of understanding that you're advocating?*
ABB: I do not have numbers. I can only give you my gut on that. My gut tells me that boards are woefully unprepared. I think the ones that are prepared are the big technology companies, which have been very avant-garde about this. The Amazons, Microsofts, Googles. They have very knowledgeable people who are well prepared for this new world we're entering. And then you might have a few others that have been working in this space. But I would say that the vast majority of the Fortune 500 probably don't have one of those people, let alone two or three.

If you are interested in contributing thought leadership or other content to this platform please contact Lester Goodman, Publisher

Follow us on Social Media

Email Me

Our Privacy Policy