An Interview on Cybersecurity with Brian Bartow, General Counsel and Chief Compliance Officer of the California State Teachers' Retirement System

By Suzanne M. Dugan

Spend some time with Brian Bartow and you'll soon learn that worrying about cybersecurity is what keeps him up at night. As the General Counsel and Chief Compliance Officer at CalSTRS, Brian is responsible for enterprise information management and security. He has even taught a law school class on the topic. Brian sat down for an interview to share his knowledge and insights about cybersecurity.

Suzanne Dugan, Cohen Milstein: How serious is the cybersecurity threat to pension systems?

Brian Bartow, CalSTRS: Except for funding, it is the number one risk we face. When you assess risk, the analysis is typically two dimensional—that is, we look at the severity of the risk and the likelihood of its occurrence. With cybersecurity risk, there is an added third dimension. In addition to severity and likelihood, we assess the velocity of the risk. If a breach happens, it's going to happen immediately, whether the breach affects one record or brings down the whole system.

Dugan: Is the risk increasing?

Bartow: Attempts to breach the system are increasing at a rapid rate. We might have had 2 or 3 attempts to redirect electronic deposits two years ago, then it jumped 30-fold last year, and we are on track to triple that this year. There is so much information now available on the dark web that malefactors can capitalize on this and create synthetic identities from which they can launch targeted attacks. This uptick was fueled by the breaches where information such as social security numbers, and health information was stolen and now can be cross-referenced with other publicly available information like name, salary and workplace. Malefactors are infinitely resourceful and very motivated. We constantly monitor data analytics so that we can identify deviations in the levels of usage of data and patterns of access, from which we develop early indicators and investigate and respond immediately.

Dugan: What steps should a pension plan be taking?

Bartow: First and foremost, the cybersecurity threat must be characterized as a fiduciary responsibility and identified as a risk so that it is brought to the board's attention. That step is critical. The board must then come up with a budgetary device recognizing that this threat constitutes an expenditure line item. Addressing the critical risk of cybersecurity requires a commitment of resources. There's no way around that.

The next step is to perform an audit, whether internal or external, looking at the existing internal controls and reporting on cybersecurity risk. This audit should lay the framework for how to address the risks. Cyber risks can fall into various categories, such as operational, financial, and reputational. Risks may come from third parties, such as employers, vendors or contractors. A cyber plan can begin to be developed from this assessment. Systems can then be developed and implemented to address the risks. Ways to manage the risks might involve purchasing cybersecurity insurance—the cost of which has come down of late—and including contractual provisions assigning risk and responsibility or providing for indemnification.

Dugan: Is there any guidance regarding best practices?

Bartow: A number of organizations, including the AICPA, National Association of Corporate Directors, the SEC and the Center for Internet Security, have begun to develop some reports that suggest ways to manage these risks. We must appreciate that the risks are ongoing and constantly evolving so that vigilance is essential. The best deterrence is knowing your data and who is touching it, as different kinds of data create different kinds of risks. Collecting information and reviewing it regularly are essential to planning and implementation.

Dugan: CalSTRS is a big fund with lots of resources. What about smaller funds with less capacity and fewer resources?

Bartow: The risks are the same for funds of any size. The appeal of the data to bad guys is the same regardless of the amount of money under management. The steps outlined here, from getting the board's attention to prioritizing these issues to assessing these risks to developing and implementing plans, are the same. It may be that resources will affect the extent of a response but should not be a barrier to an organization identifying the issue as a priority and assessing the attendant risks. Considering the operational, financial, and reputational risks, those steps are critical to fulfilling a board's fiduciary duty. ◆

Suzanne M. Dugan *is Special Counsel and leader of Cohen Milstein's Ethics and Fiduciary Counseling Practice*