A Call for a New Cyber

By Dennis Cagan

Dennis Cagan is seasoned board director, high-technology executive, and entrepreneur. Since 1968, he has served on 53 corporate boards, both private and public, predominately early and mid-stage technology companies, and he has founded or co-founded more than a dozen companies, including his first software firm in 1968. In 2013, he was honored by NACD and the Dallas Business Journal as one of 12 Outstanding Directors in North Texas. He resides in Dallas and can be contacted at dennis@caganco.com.

Over the last few years, cybersecurity risk has quickly risen to be the most dangerous, multi-dimensional risk faced by any organization. The *cyber* part of the term *cybersecurity* is fairly new, especially for companies, while the *security* part is an age-old problem for businesses. In terms of corporate governance, who has the ultimate fiduciary responsibility for this critical issue? The board, of course.

Most board discussions of cybersecurity focus on potential threats, protection and response scenarios, and questions the board should be asking. This is fine, but with the potential magnitude of this risk, proactive oversight really requires more. There are four common governance and management practices that are long overdue for change.

In 2011, as a director and the interim CEO of a cutting-edge cybersecurity software firm, I found it to be an eye-opening experience—even after over four decades in the information technology industry. I met high-level NSA and Pentagon officials, congressmen, senators, and top technology and security experts. I had run software companies before, but this was different. The urgency of the issues was frightening. The ongoing white hat (good guy) development of defensive cybersecurity software was losing ground to increasingly aggressive and well-backed black hat (bad guy) actors of all sorts. The chasm we are careening toward is global economic chaos. This situation requires an unparalleled, concentrated, cooperative, government-sponsored effort to advance state-of-the-art defensive capabilities and the ubiquitous deployment of those solutions to stave off the disastrous potential economic and social consequences.

The Origin of IT

Definition: cy·ber 'sībər/ *Adjective*, of, relating to, or characteristic of the culture of computers, information technology, and virtual reality. *Synonyms:* electronic, digital, wired, virtual, web, Internet, Net, online.

The real key here actually relates to the words wired, web, Net, online, and especially the Internet part.

In the 1960s, when what we now call information technology (IT) was referred to as data processing, almost nothing was interconnected with digital communications links, and therefore, there was little risk of information being compromised electronically from external sources. At that time, the bad guys had to physically gain access to the premises in order to steal anything; and that was a physical risk for a criminal. Today, most systems are connected to the Internet—which has brought about defining changes to information security. The Internet now delivers ubiquitous, widespread digital communications linkages between peoples, companies and governments—globally, in millionths of a second. A thief can now hack a U.S. company's digital information while sitting comfortably at an Internet café in Beijing.

This perspective is key for companies. This is not about legacy enterprise software. This is not about IT professionals focused on applications, databases, productivity, user priorities, or costs. This is not about automating operations to stay ahead of competition. A proprietary or custom solution is not even an option. No single company, especially an end-user enterprise, can afford, much less be successful, at developing the complex cutting-edge technology needed to defend against the global threats that exist today and will exponentially increase tomorrow.

In 1995, investment banking analyst J. Neil Weintraut first offered the phrase, "The Internet changes everything!" At that time, who could foresee the full implications of that statement? Today even common citizens in undeveloped countries can detail many of those implications. Few who are in business, or watch television, or read a newspaper can remain unaware of the reach or risk of Internet-borne threats. How can the existing bodies of corporate governance and organiza-

tional good practices catch up? Currently, even best-of-class companies have not adequately demonstrated their acknowledgement of the magnitude of these technological issues in fundamental ways that relate to their corporate governance and management practices.

Four Obsolete Practices

Overwhelming evidence suggests that today's enterprises will live or die based largely on IT. Computing devices of all types, the software that manipulates their circuits, and ubiquitous digital communications, are now the primary driver of operations, administration, marketing, product and service differentiation, productivity, and more. As a board comes to a fundamental understanding of this new environment, there are four key changes to historical policies that they would direct. Changes that should communicate to observers both inside and outside the company that they grasp the magnitude of the risks and rewards that electronic bytes threaten and offer. These adjustments, when combined with the best practices boards are now learning, would demonstrate the responsible fulfillment of their fiduciary duties.

To many observers, the lack of these simple changes can put the board's overall performance into question. A majority of American corporations continue to adhere to four legacy governance and management practices that are now 20 years out of date. Changing these dynamics would dramatically contribute to mitigating cybersecurity risk within a business.

1. The senior C-level technology officer should report directly to the CEO. If they do not, the company is still viewing technology in general as a tool, not core to their survival, and they therefore only put cybersecurity on par with other risks, including misalignment of financial data. When a technology officer reports to the COO, technology will be viewed as an operational tool; if reported to the CFO, technology will be viewed as a cost center and generator of data. If reported to the president, technology will be viewed on a slightly higher plane, but unless reporting is done directly to the CEO, it will not be allocated the respect and resources that will be required for the entity's survival, much less success. Until the leader of the enterprise is directly educated and informed, and buys in, no real protective or business-driving adaptations of technology can be truly successful.

2. The potential consequences of cyber risk in terms breadth, depth, and magnitude, demand a new standard of board committee oversight. Cybersecurity is a risk, of course. Therefore, with most corporate boards, oversight usually falls under the audit committee, which is typically chaired by a retired accounting firm audit partner or a retired CFO. Is cybersecurity really best assessed in a financial context only? In addition to financial risk, can this committee really understand the potential catastrophic impact on the brand, the customers, the employees, or the regulators? Does the committee have any members who possess digital credentials? It is time that risk and finance are separated and both receive the committee attention and expertise that they deserve.

3. The overriding importance of IT in business demands that boards recruit directors with appropriate qualifications. As with the audit committee, very few boards of non-technology companies contain members with IT expertise. Even sitting directors who are former high-level CEOs generally have not had direct hands-on experience managing the digital technology infrastructure that was the underpinning of their massive organizations. In today's board room, expertise from the political, educational, non-profit, financial, and C-suite sectors are well represented, yet there is little or no technology expertise—specifically broad, real-world technology experience.

4. The full board needs to directly hear from senior technology management as frequently as they do senior financial executives. I have observed that few boards get direct reports from the senior technology executive frequently enough. Many only get full technology reports once or twice a year. With the critical nature of cybersecurity, not to mention the impact of technology on operations and marketing, I believe that the board should get direct updates on a number of key issues relating to technology at every meeting. In addition, referencing the above point, when senior technical management reports through the CFO or COO, the nature of the information is generally diluted and dulled. This does a disservice to directors asking more in-depth questions, since those executives generally will not have the needed technical grasp of the issues. What board does not see financial metrics and key performance indicators at every meeting? The digital engine at the heart of producing the products, generating the financial performance and information, and protecting the enterprise's hard assets and intellectual property deserves no less.

As with all risk, the responsibility for cybersecurity risk ultimately lays with the board. The ground rules have changed for risk in general and for cybersecurity specifically. Boards that pursue best governance practices should be aggressively moving toward the policies noted above in order to fully understand the potential implications of today's risk landscape and to effectively guide management in appropriately mitigating their dangers. In general, until a company's governance and management infrastructure has adapted to and integrated today's technology challenges, the boards are not properly fulfilling their fiduciary duties.