Caremark–*and More*–Propel New Board Risks

By Raymond Hutchins and Mitch Tanenbaum
March 10, 2023

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

As detailed in the new, non-technical white paper, *The Global Cyberwar and Societal Response*[1], our society operates on top of an IT infrastructure that was never designed with security in mind. Cybercrime, a component of the global cyberwar, is a threat to our nation's financial systems, public utilities, national defense infrastructure, and health care systems. It is also a threat to most companies.

Historically, it has been virtually impossible to assess global financial losses due to cybercrime by nation states and others. Some sources have estimated that global cybercrime costs have reached $6 trillion to $7 trillion[2] annually. To put this kind of loss into context, it may be useful to note the annual GDP of the top three countries[3]: USA ($20.4 trillion), China ($13.4 trillion), Japan (5.0 trillion). Whatever the actual numbers are, it's become clear that the losses and risks are huge—and *should be alarming and unacceptable to ALL boards*.

A common problem in corporate governance is that too often boards of directors don't force executive management to do *their* jobs. With the advent of the global cyberwar, this failure is even less acceptable. But few directors know the first thing about cybersecurity and privacy–not even enough to ask relevant questions of management. This, and a lack of regulatory controls has made it difficult to hold directors' feet to the fire.

An example of just how prevalent this problem is within our business hierarchies is that Gartner, Inc. reports that only 12% of boards currently have a dedicated cybersecurity committee. Gartner goes on to predict that only 40% will establish one by 2025[4]. Again, this is an unacceptable governance statistic in this cyberwar environment.

[1] https://drive.google.com/file/d/18_hith1t5j-VmS0FNqXq6M6uR-zJY9UI/view?usp=share_link

[2] https://content.secureworks.com/-/media/Files/US/Reports/Secureworks_NC2_BoardroomCybersecurityReport.ashx?modified=20220809161846

[3] https://worldpopulationreview.com/countries/by-gdp

[4] https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk

As pointed out in the white paper referenced above, when business leaders do not act, then governments and courts are forced to act. This is happening with respect to board risk and management responsibilities.

In 2019 there was a lawsuit that established that members of boards of directors had personal liability for regulatory compliance oversight[5]. This new liability, this new responsibility, is referred to as the "Caremark Standard." Cybersecurity is a mission-critical risk, and risk management is a core responsibility of the board. The Caremark Standard establishes this and increases personal risk for board members.

Adding to regulatory compliance requirements are new rules related to boards of directors' responsibilities and company data protection requirements currently being rolled out by the Federal Trade Commission and the Securities and Exchange Commission[6].

On June 23, 2023 it was announced that the SEC had alleged that the Solar Winds CFO and CISO had violated U.S. securities laws. This is the first instance of the SEC going after company executives personally for their failure to comply. Where does the CEO fit into this situation?

Update March 10, 2023: *Report on new lawsuits driven by Caremark Standard*

On top of everything, there are new customer and insurance pressures for better risk management, new cybersecurity and privacy laws, and changes in the views of federal courts on what constitutes Article III standing[7]. It becomes clear that boards must quickly adapt to reduce *their* risks.

Of course, directors hope that they have shifted the risks of cyber liability to their Directors and Officers (D&O) policies. But insurance companies are rapidly raising rates and denying coverage to directors and boards that fail to meet their responsibilities and legal obligations. D&O insurance has become thin ice for directors evading these new responsibilities.

[5] https://corpgov.law.harvard.edu/2022/01/23/a-directors-duty-of-oversight-after-marchand-in-caremark-case/

[6] https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight

[7] https://epic.org/issues/consumer-privacy/article-iii-standing/#:~:text=Article%20III%20of%20the%20U.S.,Controversies%E2%80%9D%20arising%20under%20federal%20law.

There is much that boards of directors can quickly do to ensure that management meets its cybersecurity and privacy responsibilities. These actions can improve corporate governance, reduce risk, and ultimately increase company valuations.

Potential board governance actions include:

- Formally elevating cybersecurity and privacy to a board-level responsibility.
- Ensuring that the governance of cybersecurity privacy risk is addressed on a company-wide basis and not just as an IT matter.
- Supporting in-depth risk disclosure, which will clarify for investors and other stakeholders the rigor of the board's oversight and management's role in assessing and managing cybersecurity risks.
- Ensuring that IT and management break out of their silos and echo chambers and promote a culture of cooperation, both internally and with other organizations.
- Leading an organizational effort to correctly realign board and management financial incentives to reward cybersecurity and other risk governance activities.
- Utilizing outside parties to help expand knowledge bases, strengthen capabilities, and identify blind spots in security and risk management.

About the Authors

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies and are the authors of *The Global Cyberwar and Societal Response*

Please learn how Mitch and Ray can provide critical risk management training to your board.

https://cybersecurity-training-for-boards.com/

Ray's and Mitch's wide range of cyberwar experiences in the defense of organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/