Cybersecurity and Data Breaches: How In-House Counsel Can Engage the Board

Technology, Privacy, and eCommerce

A company's board of directors has a duty to oversee all aspects of the company's risk management efforts. This includes a duty to recognize and minimize the company's exposure to cyber attacks. In today's increasingly digital age, a company faces a variety of threats to its data — including confidential company information and sensitive customer information — from various sources, ranging from sloppy or malicious current or former employees to third party hackers. And those executing the purposeful and targeted attacks are increasingly more sophisticated, highly organized, financially-motivated criminals, rather than amateur hackers or college pranksters. Such attacks not only put valuable information at risk, but can also adversely affect a company's competitive positioning, stock price, good will, and shareholder value.

Given the role the legal department should already play in advising and directing a company's efforts with regard to protecting its data and responding to any data breach, in-house counsel are in a good position to also help facilitate the board's oversight obligations. Below are a few tips for advising and engaging the board with regard to cyber security, with some additional perspectives from Mark Sangster, vice president of marketing at eSentire, Inc., Ed Brown, vice president and general counsel at Malwarebytes, and Steve Mickelsen, senior counsel at 3Degrees Group, Inc.

Don't assume your company is immune: The first step is ensuring the board recognizes the risks. For example, a company cannot assume it is immune from cyber attacks merely because it is a midmarket company. "It is not necessarily the size of the company, but what information a company has that determines the company's risks." Sangster explains. In fact, midmarket companies are sometimes referred to as the soft underbelly of our economy because of the numerous vulnerabilities in that market segment. Midmarket companies are often targets of cyber attacks because they don't have the same resources as larger companies. A midmarket company can have important and sensitive information about itself and others, making it an equally if not more appealing target for an

attack.

Ensure the board is structured to address cyber security issues: "It is up to the board to implement cyber security culture at a company."Brown says. This effort starts with making sure the board itself can identify who on the board is responsible for taking the lead on cyber security issues. In-house counsel help identify and advocate for a designated board member to be responsible for cyber security. Then task that person with the role. If the board does not have a director with the appropriate technical expertise, this skill set should be considered for the next director vacancy. And in the meantime, a committee or subcommittee can be formed with the directors who are willing and able to learn about and embrace this key role.

Further, once the right person or committee on the board is identified, in-house counsel should make sure the board has the right liaisons with the company. The company may have a Chief Information Security Officer or similar position and/or a cross-department committee within the company with individuals tasked to address cyber security issues from various roles and perspectives within the company. The relevant board members and those company leaders should be in a position to communicate and work closely with each other.

Educate the board about the company's vulnerabilities: A key step in effective cyber security is understanding what is at risk. And from the board's point of view, it cannot embrace, lead, or oversee an issue it does not understand. Therefore, a key role for in-house counsel can be to educate the board on the company's cyber security vulnerabilities. This includes identifying the data at risk. What does the company have that others may want? Where is it? Who can access it? The board should be able to clearly articulate what information is the most valuable, and where and how that information may be vulnerable. For example, the information to be protected may include source code, personally identifiable information, money-related information (e.g. wire, escrow, credit card, or banking information), mergers and acquisition information, and important information from other third parties (e.g., partners or customers).

In addition to identifying where that information exists within the company, it is also important for the board to understand who else possesses or has access to the information. Regardless of what protections a company has in place, the information's security is only as good as a vendor's policies. For this reason, the board should help evaluate vendor relationships and conduct due diligence about a vendor's policies and practices. Also, it is also helpful to think about how the company can limit what is provided outside the company to the extent possible. Mickelsen notes, "Nobody can steal what your vendor or partner doesn't have, so a company should try to limit how its sensitive information is used and shared."

Involve the board with the plan: The board must also have a strong understanding of and involvement with the company's written plan for how its information will be protected and how the company will respond in the event of a breach. The comprehensive contents of the written plan is outside the scope of this article, but for the purposes of facilitating the board's role, several highlights should be considered:

- The board should utilize its expertise in conjunction with advice from in-house counsel to help ensure the written plan is properly tailored to the company's data, operations, industry, and the relevant legal and regulatory environment.
- The board should ensure the written plan regarding internal controls, information inventorying, and access protocols is being properly implemented.
- The board can help encourage or facilitate cyber security trainings for management or

employees, as anticipated in the plan.

- The board should determine if sufficient company resources are being allocated to the cyber security efforts, it should carefully review budgets for IT, privacy, and other cyber security efforts, and it can help allocate money if necessary to hire necessary personnel or purchase necessary equipment.
- The board can help select the vendors in advance who will help with a data breach response; for example the company should determine ahead of time who it would need to call in the event of a breach, including for technical support, customer notification, PR, and legal advice.
- The board should be involved in reviewing SEC or other regulatory disclosures regarding data security risk, to make sure the company is thoroughly addressing the risk and plan in place, without overpromising.

Having a concrete, written plan in place is key to ensuring a company understands the issues, is maximizing its preventative efforts, and can react and put its best foot forward during an attack or breach event. Cyber attacks happen fast, and there may be the need for a company-wide response within hours, or less. The board should ensure the plan is sufficient to facilitate the necessary actions well in advance of any attack.

Provide resources about applicable standards: In-house counsel can also help the board be proactive in its oversight by educating the board about applicable and evolving industry standards. For example, the National Institute of Standards and Technology ("NIST") released in 2014 its "Materials including Framework for Improving Critical Infrastructure Cybersecurity." This is a set of industry standards and best practices that is currently voluntary, but could arguably play a role in evaluating the reasonableness of the company's – and the board's – conduct and execution of duties in practice. This type of measuring stick could become relevant down the road, for example, if the directors face litigation resulting from a data breach for allegedly breaching their fiduciary duty to provide reasonable oversight with regard to the company's sensitive data.

By providing the board with this type of additional resource, in-house counsel can help the board take further ownership of its independent oversight efforts. And the more engaged and educated the board is on these issues, the better positioned it will be to evaluate and contribute to the substantive tasks of assessing risks, crafting a plan, and overseeing implementation.

Help the board maintain regular involvement, and document its efforts: The board's ability to effectively oversee cyber security issues is predicated on sufficient, ongoing involvement and information**.** "Boards are very good at recognizing patterns," according to Brown. Therefore, it makes sense to regularly share the experiences and solutions of the company and others in the industry with the board.

To help facilitate this ongoing involvement, cyber security should be a routine item on the board's agenda. The board can also help conduct periodic risk assessments, and address the results of those assessments. Any work and attention on these issues should also be documented in board minutes. Such documentation can help illustrate as necessary that the board was properly functioning in its oversight role.

Support board involvement with purchasing cyber insurance and understanding what it can and cannot cover: Although general commercial liability policies may not apply to data breach events, cyber policies can be purchased to cover costs that may arise as a result of a breach, including standard investigation costs, notice of affected clients, credit check protection, and PR costs. Mickelsen suggests, "It is important to buy comprehensive cyber insurance and to understand

what it covers and any notification requirements." While cyber insurance helps to offload some risk, it should not be counted on to offload all risks completely. The board should understand which risks may be covered, and where gaps or challenges may remain. And boards should never assume insurance will cover all the company's needs in case of an attack. For example, insurance cannot make up for resulting damage to a company's brand or core business. Insurance is helpful, but prevention is still key.

Encourage the board to be focused, but flexible: Given that methods of cyber attack are evolving constantly, so must methods of defense. Mickelsen points out, "The ground is always changing, so it is important that you are always doing the best you can. Keep in mind what is reasonable now may not be reasonable later." In-house counsel should help keep the board apprised of recent developments or trends, and can remind the board that cyber security practices must be continually improved and updated.

Sangster's cybersecurity media recommendations

Cyber-Risk Oversight Handbook
National Association of Corporate Directors

Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It
Marc Goodman

Spam Nation: The Inside Story of Organized Cybercrime from Global Epidemic to Your Front Door
Brian Krebs

Cybercrimes with Ben Hammersley
Documentary starring Ben Hammersley

Olga V. Mack

Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Carly O'Halloran Alameda

Business Litigation Partner

Farella Braun + Martel in San Francisco

Her practice includes litigating complex business disputes in CA state and federal court and alternative dispute resolution processes, and also state and federal appellate work. Her practice is complemented and enriched by her position on the BOD of Mammoth HR, a private company focused on helping businesses with HR compliance and employee management.