May 11, 2021

Cybersecurity Oversight and Defense — A Board and Management Imperative

This past weekend, criminal ransomware cyberattacks drove the shutdown of one of America's largest pipelines for refined gasoline, diesel fuel, and jet fuel as a precautionary means of containing the impact of the breach, highlighting the vulnerability of the nation's energy infrastructure. Recent reports indicate that more than two dozen other company victims across a range of industries were targeted by these ransomware attacks, with worse damage blocked thanks to close and rapid coordination between federal authorities and private sector partners to identify and swiftly shut down servers being used in the attack. Earlier this month, a California-based regional hospital operator had to take healthcare IT systems offline following a cyberattack, significantly disrupting care, forcing medical personnel to use back-up paper records and raising concerns about vulnerabilities in the healthcare system as the nation continues to battle the Covid-19 pandemic.

In addition to the most recent incidents highlighted above, 2020 featured one of the most ambitious and troubling cyberattacks in history: hackers associated with a foreign intelligence service surreptitiously implanted malicious code into Texas-based technology firm SolarWinds's Orion network management tool, an application used by tens of thousands of clients, including Microsoft, the U.S. government and FireEye, a prominent cybersecurity firm that helped discover and alert the world to the compromise. More recently, in April 2021, authorities discovered that attackers had, since at least June 2020, been exploiting security flaws in virtual private network (VPN) products offered by an IT software provider. Like the SolarWinds hack, the breach affected federal government agencies and numerous private companies.

The risk of targeted attacks from criminal groups, foreign intelligence services, and other bad actors has only increased with the mass shift to remote work arrangements, embrace of cloud-based operations and increased reliance on virtual commerce spurred by the pandemic. These recent and ongoing cyber incidents, among many others, reinforce the imperative that companies diligently consider cybersecurity risks, mitigate vulnerabilities, engage in active defense, leverage law enforcement resources and third-party specialists identified in advance, and plan for robust and rapid incident response, including from ransomware and other extortion-based attacks.

Furthermore, legal and regulatory demands on companies to safeguard sensitive data, protect against intrusions, and make related disclosures to government agencies, stockholders and the public have grown in strength and scope. Institutional

investors, proxy advisory firms and other market actors have also maintained a strong focus on public company cybersecurity oversight as part of regular shareholder engagement and escalation mechanisms, including through withhold campaigns, lower "scoring" on governance assessment tools and supporting activist campaigns in the wake of cyber incidents. Cybersecurity has also become a core component of ESG and sustainability-related frameworks and a focus of industry-specific regulators.

Governing legal principles, the highly technical nature of cybersecurity, and common sense continue to compel the proposition that the board cannot and should not be involved in day-to-day cyber risk management or be viewed as responsible for guaranteeing cybersecurity. The applicable guidance and our experience do, however, teach that boards of directors and management teams should, as a general matter, have the following in mind when it comes to cyber risk:

- Oversight Mechanism: Boards should carefully consider with management the avenues through which they monitor cyber risk. Although it is common to have the cyber risk oversight function fall to the audit committee, this should be carefully considered given the burden on audit committees. An alternative to consider, depending on the magnitude of the oversight responsibility, is the formation of a dedicated, cyber-specific board-level committee or sub-committee. At the same time, because cybersecurity considerations increasingly affect all operational decisions, they should be a recurring agenda item for full board meetings. Companies that already have standalone risk or technology committees should also consider where and how to situate cybersecurity oversight. The appointment of directors with experience in technology should be evaluated alongside board tutorials and ongoing director education on these matters.

  Robust management-level systems and reporting structures support effective board-level oversight, and enterprise-wide cybersecurity programs should be re-assessed periodically, including to ensure they flow through to individual business units and legacy assets as well as newly acquired or developed businesses. Corporate cybersecurity considerations should also extend to a company's supply chain, vendor and business partner relationships and business initiatives involving new markets, new digital platforms and material changes to business models and operational structures. Companies should also consider when and how expert third-party firms will be used as part of the company's cyber risk efforts and what kind of periodic reports and analysis, including from such firms, are provided to the board, relevant committee(s) and/or senior management.

- Review of Policies, Procedures and Resources: In carrying out their oversight function, directors should ensure that the company has written policies and procedures in place governing each of the elements outlined in the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. Both the cybersecurity and internal audit functions should be adequately resourced with respect to cyber risk-related responsibilities and include personnel with the necessary technical expertise and sufficient time to devote to cybersecurity risk and review. A review of the common elements of remedial and other cyber-related enforcement actions brought by state and federal actors suggests a growing expectation among regulators that companies maintain written information security programs that senior management present to the board on at least an annual basis.

- Verification of Risk Identification and Assessment: Companies should work to ensure that their directors have an understanding of the mission-critical systems the company uses, and the data it collects, as well as the risks the company faces by virtue of how it uses technology and stores and collects data. While managing the cybersecurity-related risks of remote work arrangements is a task that virtually every company has taken on as a result of the pandemic, each company's cyber risk profile is unique. The role of directors is to ensure that a cyber risk assessment and mitigation system is in place at the company, that those managing the company's cybersecurity identify and consider potential vulnerabilities (leveraging the latest threat intelligence and best practices), and that the board is engaged in active oversight of such matters.

- Oversight of Protection, Detection and Mitigation Plans: Directors should be briefed on management's plan for implementing appropriate protections against cyber intrusions and related risks, including programmatic efforts to detect and mitigate vulnerabilities and enable business continuity. In addition, directors and executives should maintain a sustained focus on the timely remediation of material cyber risks, whether identified by internal or external sources, and, where exposures or shortfalls are identified, confirm that appropriate protective or remedial recommendations are enacted without undue delay. Responsible personnel should be engaged in continuous monitoring and improvement efforts, including as to seemingly mundane but mission-critical tasks like timely patching of critical systems. Knowledgeable employees from the internal audit function should usually be involved as well.

- Oversight of Response Strategy and Disclosure Protocols: Directors should receive briefings from time to time on the procedures put in place by management to facilitate a swift, robust, and effective response to a breach or other cybersecurity incident. A company's response plan should cover all categories of likely incident scenarios, as well as unlikely but plausible scenarios with extreme consequences. The plan should address notification and response protocols, procedures for escalation to appropriate management personnel and ultimately the board, business and service interruption scenarios (including whether such steps could be taken as a precautionary measure following an identified breach) and communications with regulators and stakeholders. The company should also have a coherent and legally vetted plan for making appropriate and compliant disclosures and notifications if systems are materially compromised.

  The board should also expect to be appropriately briefed on the company's response to material cybersecurity incidents and related impacts, the status of material investigations, whether the company's response plan worked effectively in practice and whether management recommends material changes to the response plan and the company's cybersecurity systems following a significant incident.

- Documentation of Board-Level Oversight: Finally, board and committee oversight activities, including in the aftermath of a material cyber incident that causes significant harm or disruption, should be appropriately documented in minutes and in supporting materials. Stockholder inspection demands to review a company's books and records, including board- and committee-level minutes, in preparation for litigation are increasingly common and allowed by the courts where legal requirements are met.

Adhering to these principles will not eliminate cybersecurity risks. They also will not reduce the continuing need for coordinated federal, state, and local enforcement and policy responses, intensified industry-level action, effective public and private sector collaboration, and global action on these issues. Rather, these concepts offer a solid foundation for an effective board-level oversight posture with respect to the growing scale of cybersecurity risks.

John F. Savarese
Sarah K. Eddy
Sabastian V. Niles
Jeohn Salone Favors