ALERT MEMORANDUM

Cybersecurity in the Age of Cyber Warfare: Governance Reminders for Public Company Boards

March 23, 2026

Just a few days ago, a state-linked hacking group claimed responsibility for a disruptive cyberattack on a Fortune 500 medical technology company with no ransom demand and no negotiation, calling it retaliation for a U.S. military strike. The risk of this type of politically-motivated cyberattack may increase given the increasingly volatile geopolitical environment. To combat this, the President recently signed an executive order targeting cybercrime carried out by transnational criminal organizations, aimed at improving federal coordination in combatting cybercrime. Now is an important time for boards and management teams to focus on crisis and risk management, including durable operational resilience planning. This alert provides perspectives about current best practices on incident preparedness in the face of such threats, explains how this preparedness can be supplemented by an operational resilience framework, discusses the practical implications of the executive order, and lays out a governance hygiene checklist to guide your next cybersecurity oversight discussion.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Lillian Tsu
+1 212 225 2130
ltsu@cgsh.com

Francesca L. Odell
+1 212 225 2130
flodell@cgsh.com

Synne D. Chapman
+1 212 225 2374
schapman@cgsh.com

Shuangjun Wang
+1 212 225 2451
shwang@cgsh.com

Breon S. Peace
+1 212 225 2052
bpeace@cgsh.com

Victor L. Hou
+1 212 225 2609
vhou@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Lisa Vicens
+1 212 225 2524
evicens@cgsh.com

Bobby Bee
+1 212 225 2523
rbee@cgsh.com

SAN FRANCISCO

J.T. Ho
+1 415 796 4495
jtho@cgsh.com

Marcela Robledo
+1 415 796 4450
mrobledo@cgsh.com

SILICON VALLEY

Jennifer Kennedy Park
+1 650 815 4130
jkpark@cgsh.com

Board and Management Obligations: The Caremark Dimension

Under Delaware's Caremark framework, directors' fiduciary duties require reasonable oversight of the company's affairs. Liability may follow if directors either "utterly" fail to implement any reporting or information systems or controls to monitor or oversee "mission-critical" risks, or, having implemented such systems, consciously fail to monitor or oversee such risks.

Cybersecurity qualifies as a mission-critical risk for many companies today, and boards should ensure that reliable reporting systems exist for it. Boards that receive red flags, whether from internal employees, auditors, or third-party assessments, and do not respond could face meaningful legal exposure. As part of their oversight, boards should periodically confirm that no material red flags have gone unaddressed by management, and that employees know how to raise concerns through clearly defined escalation thresholds and mechanisms. Ignoring these issues can be seen as both a governance failure and create litigation risk. Corporate documentation, including board minutes, board books, and other formal records should reflect the information the board receives and the decisions it makes. Conversely, the absence of any cybersecurity discussion in meeting minutes could create an inference at the pleading stage that the board never addressed the topic at all.

With those obligations in mind, the following sections outline practical steps companies can take to better prepare for an eventual incident.

Don't Wait For The Incident

Most public companies already conduct cybersecurity risk assessments and maintain an incident response plan, but the current threat landscape warrants a fresh look. Existing assessments should expand to account for state-actor threats, reviewing systems and software for vulnerabilities that a politically motivated attacker might exploit, auditing code, identifying unpatched software, and stress-testing third-party dependencies. The goal should be to ensure that the risk assessment keeps pace with a threat environment in which adversaries are pursuing disruption or espionage, unconstrained by financial motive.

Tabletop exercises remain one of the most practical tools available. Companies already running tabletops should update their scenarios to include state-actor attacks aimed at prolonged disruption or espionage, not ransom. The exercise should test whether one point of infiltration can impact a significant portion of the network or if the organization can shut down affected systems, reroute operations, and recover within a defined timeframe. Tabletop planning should also cover what happens during a prolonged outage, not just how to end it.

Stakeholder communications deserve specific attention. During a sustained disruption, employees, vendors, customers, and regulators will seek information, often simultaneously. Some communications carry legal or contractual obligations; others can inadvertently trigger public disclosure, and there may be deadlines associated with required notices. Companies that map their stakeholder communication sequence in advance may avoid reactive, ad hoc outreach during a crisis.

Potential financial impact also warrants advance planning. Whether an incident crosses the materiality threshold for SEC disclosure turns in part on its financial consequences. Companies that model that potential impact prior to an incident, including under scenarios where core systems stay offline for days, may make more defensible disclosure decisions under pressure.

Operational continuity planning rounds out the picture. Some companies have fallen back on manual processes, such as taking orders by hand, to keep critical functions moving during an attack. Manual workarounds can bridge a short gap, but they do not scale. Companies should identify their most critical functions and confirm whether tested fallbacks exist that do not depend on primary systems, updating that assessment as operations and threats evolve.

Companies should also confirm that their incident response and/or crisis management plans are kept up to

date to reflect current trends and fresh messaging. A stale document may offer little value when the clock starts running. For best practices on crisis management protocols, including for cybersecurity and data privacy incidents, see Cleary's Global Crisis Management Handbook.

Think Resilience, Not Just Risk Management

Traditional risk management planning centers on control and prevention: identifying specific threats, quantifying their probability and impact, and putting mitigation strategies in place. This approach can sometimes fall short when a state actor has the capability to disrupt a company's systems overnight, particularly when that threat actor has no interest in negotiation or compensation. Unlike a ransomware attack, where a company can at least evaluate whether to pay a ransom, a purely disruptive or espionage-driven attack offers no immediate pathway to resolution and no shortcut to recovery. That is where operational resilience planning comes into play, supplementing traditional risk management with a focus on sustaining operations amid disruptions. No organization can prevent every cybersecurity incident, but companies that invest in data redundancy, segmented network architectures, and rapid-recovery capabilities stand a far better chance of weathering a cybersecurity attack than those that rely primarily on perimeter defenses. An attack that wipes employee devices can take supply chain management and customer ordering systems offline entirely. Boards should consider asking management whether the company has mapped its most critical functions, confirmed that tested fallbacks exist for each, and committed to updating that assessment as operations and threats evolve.

Build Your Response Network

Companies should identify and engage their external advisors well in advance, including outside counsel with expertise spanning corporate governance, SEC disclosure and reporting, white-collar defense and regulatory enforcement, data privacy, and cybersecurity investigations, as well as a cybersecurity forensics firm and a crisis communications firm. Internal roles should be clearly defined, and all members of the response team, both internal and external, should know who the other members are, and understand their respective roles and responsibilities.

Companies should also establish a relationship with their local FBI office before a cybersecurity incident occurs. Early engagement with law enforcement can support a company's ability to request a delay in public disclosure of a material cybersecurity incident for national security or public safety reasons. Early engagement may also assist in asset recovery in a ransomware situation, and can provide access to threat intelligence that helps the company assess risks during an incident response or prepare for emerging threats.

Monitor Third-Party Exposure, Including AI

Vulnerabilities in third-party providers represent a significant source of risk, which can be underestimated even in otherwise robust cybersecurity risk assessments. Companies should continually monitor the cybersecurity preparedness of their critical vendors—including cloud platforms, data-sharing tools, and, increasingly, AI tool providers. A state actor that compromises a significant AI implementation could gain a backdoor into an organization, whether to disrupt operations, harvest proprietary data, or both.

Internal AI use introduces its own risks. The use of unauthorized, "shadow AI", as well as the growing practice of using AI to generate production code (sometimes called "vibe coding") has already triggered internal cybersecurity incidents at companies that deployed AI-written code without adequate review. Boards should ensure that management has clear policies governing how employees use AI tools and what guardrails apply to AI-generated outputs used in code development.

Prepare for Post-Incident Inquiries

Companies should also be prepared to respond to inquiries after a cyber event. SEC staff and auditors may request explanations of the company's materiality analysis and probe for material weaknesses in internal controls. Customers will also demand information, and their requests will vary in scope and intensity.

Companies should plan for what can be shared with different stakeholders, bearing in mind that anything communicated, even under nondisclosure protections, may ultimately surface elsewhere.

The New Executive Order: Expect Government Outreach

On March 6, 2026, the President signed an executive order targeting cybercrime carried out by transnational criminal organizations, many of which operate with foreign state support. The action plan required under the order describes how the government will use "operational insights from commercial cybersecurity firms and other non-Federal entities: to enhance attribution, tracking, and disruption of malicious cyber actors." In practical terms, companies, particularly those recently impacted by a cyber incident, should anticipate increased government requests for information and cooperation. Now is the time for companies to review information-sharing policies and ensure that any agreements with third-party providers clearly define what those parties can share with the government.

Government contractors face particular exposure. A cyber breach may trigger obligations under those contracts and invite more scrutiny than what commercial clients may demand. The executive order's focus on hardening the nation's financial and digital systems and coordinating enforcement across agencies could amplify this exposure, particularly for contractors already subject to cybersecurity certifications and representations. Contractors should also be mindful of potential False Claims Act liability if cybersecurity representations made in connection with government contracts prove inaccurate or inadequately supported.

Key Takeaways: A Governance Hygiene Checklist

The below checklist is a starting point to consider for a cybersecurity risk oversight discussion.

- Do your minutes and formal records reflect the cybersecurity information the board and/or appropriate oversight committees receive and the decisions they make?
- Does the board have access to independent cybersecurity expertise, whether through a qualified director or external advisors?
- Do employees have a clear, functioning channel to escalate potential vulnerabilities internally, and does leadership appropriately respond?
- Are significant risks and appropriate mitigation steps being reported up to the board?
- Have you conducted a recent risk assessment covering your systems, code, and third-party providers, including your AI tools?
- Do your tabletop exercises include a state-actor scenario focused on prolonged disruption and espionage, not just ransom?
- Have you assessed your systems for adequate data and operational redundancy, segmented network architectures, and rapid-recovery capabilities?
- Has the board confirmed that the company's operational continuity planning, including tested fallbacks for critical functions, is reviewed and updated regularly?
- Has the company modeled the financial impact of a prolonged outage, including the effect on any materiality determination?
- Do your incident response and/or crisis management plans and disclosure controls and procedures reflect current cyber incident protocols and requirements?
- Have you identified and retained your incident advisory team (e.g., legal, forensics, and crisis communications)?
- Have you reviewed your cyber insurance coverage, including whether you should seek additional coverage and how any war exclusions or state-actor carve-outs may limit recovery?
- Do you have an open line of communication with your local FBI office?

— Has your team assessed the cybersecurity risks introduced by AI?

— Have you reviewed your third-party contracts to understand:

  • your obligations to notify any customers or partners in the event of a cyberattack?

  • your vendors' obligations to you in the event they are subject to a cyberattack?

  • what information your vendors can share with the government, including what information you may be obligated to share with those vendors?

— Are you continuing to monitor your vendors after they have been retained, including in respect of their cybersecurity exposure?

— Have you mapped what you can and cannot share with customers in the event of an incident?

— Have you mapped applicable sector-specific cybersecurity incident reporting obligations, including those imposed by CISA, sector regulators (NERC CIP, TSA, HHS), and non-U.S. regimes such as the EU's NIS2 Directive, and integrated them into your incident response plan?

— Are your processes designed to prepare you for SEC staff and auditor inquiries regarding materiality determinations and internal controls?

Cleary Gottlieb's capital markets, corporate governance, crisis management, governmental investigations, white-collar defense, AI and cybersecurity teams regularly advise boards and management on cyber risk preparedness, incident response, regulatory investigations, and disclosure obligations. For questions about any of the topics discussed above, please contact your regular Cleary contacts.

…

CLEARY GOTTLIEB