THE AUGUSTA GROUP

Securities and Exchange Commission: Cybersecurity risk management, strategy, governance, and incident disclosure

Implications for the board rooms of public firms on US Capital Markets

April 2022

Now is the time for public firms to prepare for cybersecurity risk management compliance.

Cybersecurity risk management is slowly being recognised as a significant issue by many governments, that are turning to legislation and regulatory enforcement regimes to enforce cybersecurity compliance. Recent cyberattacks including those on SolarWinds, JBS Meat, Kaseya, Colonial Pipeline and Toyota have demonstrated the impact of cyber on supply chains; the average cost of a cyber-attack increased in 2021 to $4.24 million, from $3.86 million in 2020; 2021 saw the rise of ransomware as the predominant cyber threat confronting businesses of all sizes; cyber-insurance costs are increasing, coverage is falling and insurers are adding policy exclusions or cancelling policies altogether if they cover the Ukraine Russia conflict; and the recent cyberattacks on Electronic Arts, Microsoft, Samsung, Ubisoft, Nvidia and Okta by the Lapsus$ group demonstrated that script kiddies can successfully disrupt major brands.

Cyber-related incidents were once extremely rare events. However in risk language, the likelihood of a cyber-attack for many companies has moved much closer to '1', than '0' (probability of 1, it will happen). Losses from cyberattacks could once be considered extreme loss events, with minimal financial loss using Distributed Denial of Service (DDoS) attacks. In 2021 cyberattacks were significantly more complex, frequent and the predominant cyber threat was from ransomware, capable of inflicting direct corporate financial losses of $10s millions. Costs that include ransomware payments, remediation costs, lost current and future sales, cybersecurity implementation costs, and increasingly legal costs that include class action lawsuits for data breaches. For public companies lawsuits addressing the impact on shareholder value through brand, reputation and share price are increasing. For Critical National Infrastructure (CNI) providers cyberattacks create broader risks for society. For example a cyber-attack on a power generator can have a catastrophic impact on other CNI providers such as water, financial services, health, transportation, pharmaceuticals, defense, and food production.

It has long been thought that the public and private sector can address cybersecurity risk through market forces. Allowing the board room to manage cybersecurity risk, as they manage any other critical enterprise-wide risk. But the significant supply chain hacks of 2020 and 2021 demonstrated to many that market forces alone are not working, highlighting that the public and private sector have not focused enough effort on cyber-supply chain risk management (C-SCRM). In the U.S. this resulted in the signing of Executive Order 14017 '*Americas Supply Chains* - February 2021', and Executive Order 14028 '*Improving the Nation's Cybersecurity* - May 2021'. Setting the direction of travel for U.S. cybersecurity and cyber-risk management legislation and regulatory enforcement for 2022 and beyond.

In what is a response to the increase in cyberattacks and the risk of cybersecurity incidents on the US economy and market registrants, the Securities and Exchange Commission (SEC) proposed amendments to its rules on 9th March 2022. Formalizing disclosure of cybersecurity risk management, strategy, governance, and incident reporting by boards of U.S. public registrants. The proposal, if implemented will require registrants to formally disclose;

- Policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation.
- The board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies.
- Whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise.
- Material cybersecurity incidents within four business days.

- Updates in periodic reports about previously reported cybersecurity incidents.

This is a significant update by the SEC on cybersecurity, risk management and governance. It will have a major impact on registrants who require access to capital on U.S. markets. Why?

1. The proposal applies to all registrants on SEC covered markets, irrespective of their industry sector. Whereas U.S. legislation and regulation has mainly impacted Federal Agencies and critical National Infrastructure Providers.
2. The proposal impacts foreign issuers. Extending the scope of compliance across international borders, that has similarities to the 2002 Sarbanes Oxley regime.
3. Registrants will have to implement a cybersecurity risk management program, policies and procedures that evolve with its business strategy and financial performance. This will require registrants to implement a risk management framework that includes appropriate cybersecurity practices, risk mitigation and governance.
4. Legal, Regulatory and Compliance risks will increase. Board disclosures will be scrutinized by investors and other market participants.
5. Corporate boards will have to demonstrate they are managing cybersecurity risks.
6. Board members will have to publicly report their experience and competencies to oversight and assure cybersecurity.
7. Organisations will have to report material cyber incidents and provide regular updates on incident and cybersecurity risk mitigation to market participants.

If the proposal moves ahead which is highly likely, boards of market registrants should carefully consider its impact. It will provide timely and relevant disclosure to investors and other market participants such as financial analysts, investment advisers and portfolio managers. Enabling them to assess the implications of cybersecurity maturity, risk management, board oversight and assurance, and the possible effects of a material cybersecurity incident on short and long term financial and operational performance. That are likely to have a direct impact on credit ratings (cost of capital), cyber insurance premiums and share price.

The proposal will provide market data that could increase legal and compliance risk. In October 2021 the US Department of Justice (DoJ) announced its Civil Cyber Fraud Initiative. Making it clear that organisations that supply Federal Agencies could be fined under the False Claims Act (FCA) if they fail to meet expected cybersecurity standards under contract. The first round of disclosure will generate market conversations and could result in investigations from the DoJ or the SEC. For example, defence contractors that have reported high NIST compliance scores required under US DoD DFARS regulations, or the first CMMC assessments carried out to complete DoD contracts may find themselves managing variances in SEC reporting.

CyberSecurity risk management disclosures may also be useful for civil litigation. Companies that are unfortunate enough to suffer a cybersecurity incident may find that their cybersecurity risk management, strategy, and governance disclosures are used to challenge their cybersecurity maturity, reported to the SEC over a number of years.

For those that have not read the proposal I would strongly recommend that your do. While it may not end up looking the exactly same when it is finalized, it is highly likely to be implemented and for the defense industry create additional regulatory and compliance burden, and legal risk.

https://www.sec.gov/rules/proposed/2022/33-11038.pdf