ADDRESSING CYBERSECURITY THEATS: STAY TUNED FOR NEW RULES AND/OR UPDATED GUIDANCE FROM THE SEC

Following the announcement last summer of enforcement actions relating to cybersecurity, there was an expectation that further guidance or rulemaking from the Securities and Exchange Commission ("SEC") in respect of cybersecurity risks was on the horizon. In a speech delivered today by SEC Chair Gary Gensler, we have a roadmap for possible additional guidance or rulemaking relating to cybersecurity. We, however, do not yet know the timing. My sense is that it will be sooner than later.

The focus on cybersecurity threats is not merely an exercise in disclosure or governance, but rather a recognition that the private sector has a significant role to play in safeguarding the nation's critical infrastructure. In May 2021, President Biden issued an executive order on improving the country's cybersecurity, which, among other things, called on government to partner with the private sector to protect the country from malicious cyber actors and called on the private sector to adapt to the changing threat environment, ensure its products are built and operate securely and partner with the government to foster a more secure cyberspace. In August, the Cybersecurity & Infrastructure Security Agency ("CISA") announced the formation of the Joint Cyber Defense Collaborative (JCDC) as part of an effort to integrate government and private sector efforts to address the most serious cyber threats to the United States.

The threat is viewed as only getting worse. As recently as January 11, 2022, CISA issued an alert on understanding and mitigating Russian state-sponsored cyber threats to US critical infrastructure. A potential invasion of Ukraine by Russia, followed by US sanctions, could ramp up the cyber threat significantly given Russia's asymmetrical warfare doctrine. This afternoon, it was reported that a DHS Intelligence and Analysis bulletin (dated January 23), sent to critical infrastructure operations and state/local governments, warned of an elevated risk of cyberattacks directed against the United States due to the Russia-Ukraine situation.

As for the SEC, it has two roles to play in the cybersecurity arena, one that flows from its oversight role of exchanges, broker-dealers, investment advisers and investment funds, and a second that flows from its mandate to ensure that investors and the marketplace benefit from full and transparent disclosure by SEC reporting companies. In his speech today, Chair Gensler noted that the SEC is working with a range of other bodies, including CISA and the Federal Bureau of Investigation, as part of a broader whole of government response to cyber threats.

Prior Guidance

In 2011, the SEC issued interpretive guidance (CF Disclosure Guidance: Topic No. 2) in respect of cybersecurity risks and cyber incidents. The guidance did not create new law or new obligations, but rather served as a reminder that a number of existing disclosure requirements may impose obligations on reporting companies to disclose cybersecurity risks and cyber incidents. These include the usual litany of disclosure requirements: risk factors, business section, MD&A, legal proceedings and financial statement disclosures, either prior to a cyber incident or during/after a cyber incident. These requirements also include the maintenance of effective disclosure controls and procedures.

In 2018, the SEC published a Commission Statement and Guidance on reporting company cybersecurity disclosure. The 2018 guidance was presented as reinforcing and expanding on the 2011 guidance, and also addressed two new topics: the importance of cybersecurity policies and procedures, and the application of insider trading prohibitions in the context of cybersecurity incidents.

In spring 2021, the SEC staff went on record that it was considering amendments to enhance issuer disclosures regarding cybersecurity risk governance. In the fall, it also referred to consideration of enhancements to fund and investment adviser disclosures and governance relating to cybersecurity risks.

Enforcement

Last summer the SEC announced three actions against eight broker-dealers and/or investment advisers arising from cybersecurity incidents. These followed settled charges against First American Financial Corporation relating to disclosure controls and procedures and Pearson plc relating to disclosure controls and procedures and misleading statements made to investors in respect of a cyber incident. Last summer, the SEC staff undertook an investigation regarding the attack that compromised software made by SolarWinds by requesting voluntary submissions from those the staff believed may have been affected by the attack.

January 24 Speech

Today's speech focused on four different silos: financial sector players that are registered with the SEC; SEC reporting companies; service provides that work with SEC financial sector registrants, but may not themselves be registered with the SEC; and the SEC itself. In his speech, Chair Gensler called out not only the economic cost of cyberattacks, but also the national security implications, referencing the current situation at the Ukraine border.

The key takeaways from the speech are:

- the SEC will repropose whether to extend Regulations ATS (Alternative Trading Systems) and SCI (Systems Compliance and Integrity) to alternative trading systems that trade in government securities as well as repurchase/reverse repurchase agreements on government securities (initially proposed in 2020);
- Chair Gensler believes there are opportunities to amend Regulation SCI to enhance the cyber hygiene of important financial market players;
- Chair Gensler has asked the staff to make recommendations on how to strengthen cybersecurity hygiene and incident reporting by investment companies, investment advisers and broker-dealers, beyond those covered by Regulation SCI;
- Chair Gensler has asked the staff to make recommendations to modernize and expand Regulation S-P (Privacy of Consumer Financial Information) in respect of notifications to clients and customers about cybersecurity events when their data has been accessed;
- as for SEC reporting companies, Chair Gensler has asked for staff recommendations around cybersecurity practices and cyber risk disclosure, which may include governance, strategy and risk management of cyber threats. He references presenting

information in a "consistent, comparable and decision-useful manner" and as well as calling for recommendations around whether and how reporting companies should update their disclosures when cybersecurity events have occurred; and

- perhaps the most far reaching, Chair Gensler has asked the staff to consider recommendations addressing cybersecurity risk that arises from vulnerabilities of entities providing services to the financial sector. These entities, which could include investor reporting systems and providers, middle-office service providers, fund administrators, index providers, custodians, data analytics, trading and order management, and pricing and other data services, may well not be SEC registered. Chair Gensler indicated these measures might include requiring disclosure by certain registrants of their service providers that could pose such risk or holding registrants accountable for service providers' cybersecurity measures. He noted that there is precedent: banking agencies regulate and supervise certain third party service providers to banks under the Bank Service Company Act, and it may "be worthwhile [for Congress] to consider similar authorities for market regulators."

Concluding Thoughts

None of the foregoing should come as a surprise. The SEC, as well as the national security apparatus and law enforcement, has been focused on the evolving risks posed by technology for some time. In November, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve and the Office of the Comptroller of the Currency issued a final rule on notification of certain cybersecurity breaches by banking organizations and bank service providers. The potentially widening scope of cyberattacks, as illustrated by the SolarWinds attack, has significant implications for the direct targets of the attacks, others in the information technology supply chain, those whose data are compromised as a result of the attacks and the markets.

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
January 24, 2022