SHARPE MANAGEMENT CONSULTING LLC

June 5, 2023

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

RE: File Number, S7-06-23, Comments on Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents

Dear Secretary Countryman:

Last year, Shiva Rajagopal and I responded to File Number S7-09-22, entitled "Comments on the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." A PDF of the response is attached for your convenience. Shiva leads the Corporate Governance and Cybersecurity programs for Columbia Business School.

In principle, we agree with the spirit and intent of the proposed rule changes. We believe a few modifications will make the proposed rules more palatable and improve national security. The proposed enhancements are listed below. The thought behind each is mapped out in subsequent paragraphs.

1. Exposing an organization's weaknesses before dealing with them can cause more harm than good.
2. A review by Federal Law Enforcement, Homeland Security, and the Intelligence Community will go a long way toward adequately triaging and crafting a holistic response.
3. The proposed four-day formal notice requirement is not practical. An informal notice followed by something more formal in thirty calendar days is more practical.

We suggest future updates focus on Operational Resilience (OR) and Third-Party Risk Management (TPRM).

General Comments.

24 E. Main St., #5264
Clinton, NJ 08809
Voice: 908.319.3650
eFax: 877.254.9654
alex@SharpeLLC.com
www.SharpeLLC.com

In our response to File Number S7-09-22, Comments on the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, expressed the need for regulation that addresses all three of the SEC's mission and covers all market participants, whether privately held or publicly traded. These previously proposed rule changes combined with these appear to address our concerns. Thank you.

The proposed rules demonstrate an understanding of the problem and provide a path toward increasing the cyber resilience of organizations across all three of the SEC's missions:

(i) protect investors;
(ii) maintain fair, orderly, and efficient markets; and
(iii) facilitate capital formation.

The proposed rules are aligned with the recently released "National Cybersecurity Strategy" by the Office of the National Cyber Director, The White House. The increased transparency will leverage market forces to reward organizations with better cyber hygiene.

Historically, Cybersecurity has relied heavily on technical controls and has remained the responsibility of an organization's Information Technology (IT) group. These proposed rules are a step towards recognizing that Cybersecurity is a board responsibility and part of the decision process of both shareholders and stakeholders. The proposed rules are also a step towards acknowledging that technical controls are insufficient. Going forward, we need an increased emphasis on the people, process, and organizational dimensions.

Historically, contemporary thinking was that an organization could fend off cyber-attacks. Recent years have caused industry recognition that incidents happen. The key is to design the organization to limit an incident's breadth (blast radius), contain, triage, and respond quickly. It would be good to fold this philosophy into the proposed rule changes.

Exposing an organization's weakness too soon can cause more harm than good.

Our primary concern with the proposed rules is an issue we raised in our previous response to File Number S7-09-22. We cannot forget our most ardent adversaries actively review Open Source Intelligence (OSINT), including SEC filings. Providing too much insight into an organization's weaknesses before correcting them is asking for trouble.

At the very least, we could communicate to an adversary what we have detected and, worse, what we have not. A balance needs to be achieved between transparency and helping the bad guys. The proposed rules aim to increase cyber resilience, not to help the bad guys.

24 E. Main St., #5264
Clinton, NJ 08809
Voice: 908.319.3650
eFax: 877.254.9654
alex@SharpeLLC.com
www.SharpeLLC.com

We propose organizations provide an informal notice allowing Federal Law Enforcement, Homeland Security, and the Intelligence Community. This review would go a long way towards managing systemic risk and providing for a whole Government response against bad actors if required.

A review by Federal Law Enforcement, Homeland Security, and the Intelligence Community.

Due to national security, the organization's safety, and customer safety, we believe there needs to be a review by Federal Law Enforcement, Homeland Security, and possibly members of the Intelligence Community before making a public disclosure.

The purpose of this review is to:

- understand how the reported incident fits into the bigger picture (e.g., a systemic risk or an isolated incident);
- determine what warnings are required across sectors (potentially more than just finance);
- understand the threat (e.g., Nation State, cyber kiddie);
- determine if a national or international response is required.

The four-day rule is not practical.

Stakeholders, shareholders, and the market, in general, are best served by an informal notice followed by a formal notice within, say, 30 calendar days. When it first learns of a cyber incident, an organization rarely understands what it is dealing with. The proposed rules, as written, could make the situation worse note better; official reporting will consume time and energy better applied to containing and triaging the incident. A change to the proposed four-day rule will also provide a runway for the review by Federal Law Enforcement, Homeland Security, and the Intelligence Community mentioned above.

Future Versions.

The proposed rules are focused mainly on the organization itself, and it reads as if the organization is secure. Organizations are part of an ecosystem. What affects one can affect other members. We also run the risk of aggregating risk and the contagion discussed in the proposed rules. Cyber incidents are a fact of the modern business world. We can no longer stop and recover when an incident occurs. Instead, organizations must withstand, adapt to, and recover from disruptions while maintaining business operations.

We suggest future updates focus on Operational Resilience (OR) and Third-Party Risk Management (TPRM). We recommend the SEC consider the Operational Resilience

24 E. Main St., #5264
Clinton, NJ 08809
Voice: 908.319.3650
eFax: 877.254.9654
alex@SharpeLLC.com
www.SharpeLLC.com

Framework (ORF) under development under the auspices of the Global Resilience Federation (GRF). It is a multinational, cross-sector, all-hazard initiative gaining acceptance, mainly in Financial Services. It can be found here: https://www.grf.org/orf.

Closing.

We are very encouraged to see many of our suggestions for File Number S7-09-22 incorporated into this set of rules. We believe the proposed rules are a step towards increasing the cyber resilience of the sector, which will, in turn, improve overall national security. We hope you find our suggestions helpful. Feel free to contact either of us using the information below. Anything we can do to help?

Cheers,

Alex Sharpe

Alex Sharpe
Principal
Sharpe Management Consulting LLC
alex@SharpeLLC.com
(908) 319-3650
https://www.linkedin.com/in/alex-sharpe-3rd/

Columbia Business School
AT THE VERY CENTER OF BUSINESS™

Columbia University
Graduate School of Business
Uris Hall, 3022 Broadway, Room 610
New York, NY 10027-6902
Ph: 206 724 6056
Fax: 212 316 9219
sr3269@gsb.columbia.edu

Shivaram Rajgopal
Roy Bernard Kester and T.W. Byrnes
Professor of Accounting and Auditing

To
Securities and Exchange Commission
100 F Street NE,
Washington, DC 20549-1090.

May 9, 2022

Re: File Number S7-09-22, Comments on the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Sir/Madam:

Congratulations on proposing extensive disclosure requirements related to cyber risk. To frame our comments, it is useful to summarize what the rule asks for:

- The rule requires current reporting about material cybersecurity incidents on Form 8-Ks within four business days;
- The rule requires periodic disclosures regarding, among other things:
  - A firm's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
- The rule asks for updates about previously reported material cybersecurity incidents.

We support the new requirements in principle. However, we believe these requirements do not go far enough in certain areas and can be refined in others. We also believe that the rules need to be expanded to address all three of the Commission's roles. As written, the proposed changes are highly focused on near term aspects of protecting investors (the first role): (i) protect investors; (ii) maintain fair, orderly, and efficient markets; and (iii) facilitate capital formation.

Our letter is organized in two parts. The first part provides data points to support the SEC's proposed rules. The second part lays out where the SEC could go farther with respect to the disclosure requirements.

1.0 In defense of the proposed rules

1.1 Defending the four-day disclosure requirement

Marriott waited 11 weeks to reveal that 383 million customer records had been compromised, exposing at least 25 million passport numbers and 8 million payment cards. Can you imagine Marriott waiting for 11 weeks to disclose its quarterly earnings numbers? That would not be acceptable. So, why is waiting that long to disclose a cyber incident acceptable?[1]

The data breach was noticed on September 8, 2018. Marriott filed the 10-Q covering the period ending September 30, 2018 on November 6, 2018. Although Marriott devoted two full paragraphs to the threat of cyberattacks in this filing, there is no mention of the massive data breach nor any disclosure of any economic impact to the company. Marriott then filed a form 8-K on November 30, 2018, disclosing the cyber-attack. A form 8-K is supposed to be filed within three days of the relevant material corporate event and for other types of news the company is capable of acting quickly. For example, when Senator Mitt Romney resigned from the board of Marriott on November 8, 2018, a Form 8-K was filed on November 9, 2018.

We restricted our review of the disclosures before the attack happened. Marriott's cyber disclosures mechanically improved after the attack but the whole point about disclosure regulation is to assist the investor with ex-ante assessment of the risk and return implications of cyber threat exposure.

1.2 Cyber hacks increasingly move stock prices but news is incomplete and reaches the market late

In the early days, stock prices barely reacted to a cyber hack, partly because losses were socialized among consumers, credit card companies and banks.[2] However, systematic evidence is beginning to build suggesting that stock prices move in response to news of cyber hacks, especially as more recent attacks involve ransomware. Kamiya et al (2021) find a statistically significant negative stock price reaction. In aggregate, they find that for a subset of 75 first-time attacks with negative abnormal stock returns, the total shareholder wealth loss is $104 billion.[3]

We hasten to point out that the Kamiya et al (2021) study can only track publicly revealed news of cyber-attacks. We can confidently conjecture that several cyber hacks on public firms were not revealed to the stock market. On top of that, we conjecture that the market found about these attacks many days or weeks after the breach actually occurred. Surely, the investor deserves to know in a timely manner after a cyber hack whether an attack occurred and the extent of the damage caused.

Missing or incomplete disclosures about the actual loss associated with IP (intellectual property) theft, the investment of the firm in IT (information technology) structure, dollar value of business interruption, and continuity planning, listed in 2.2 to 2.5 below, lead us to conclude that the stock price reactions documented in Kamiya et al (2021) are likely under-stated and incomplete.

The point being, stock markets and investors, are relatively in the dark, both in terms of the timing of the cyber attack and information about how to model the likely loss a public firm will suffer. The SEC's new rules would go a long way in making stock markets more efficient by addressing this gaping information asymmetry problem between the firm's management and its investors.

---

[1] Rajgopal and Gezer, Harvard Business Review, March 5, 2019. Available at https://hbr.org/2019/03/the-marriott-breach-shows-just-how-inadequate-cyber-risk-disclosures-are

[2] Rajgopal and Srinivasan, Wall Street Journal, October 3, 2016. Available at https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-was-hacked-1475537076

[3] Kamiyaa et al. (2021), Journal of Financial Economics, March 2021, 139(3): 719-749.

2.0 New requirements advocating going further

We now turn to gaps that the SEC's rules do not explicitly cover:

2.1 Expanded report aligned with all three roles of the SEC

The four-day period is a good step forward but may not be practical. We suggest that this rule be enhanced to better align with the SEC's stated objectives. We propose a less formal notice within four days with a more formal response to follow in not less than ten days and in no more than thirty days. This revised procedure will lead to a report that other firms can use to bolster their own defenses and allow the organization to address the incident at hand.

We also propose Law Enforcement and possibly other bodies such as Homeland Security be consulted before any public disclosures are made. Such a procedure would avoid compromising other deterrence efforts and foster a national (and potentially global response), as required.

In practice, cyber incidents are rarely fully understood in the short term. Rather the full impact and understanding of the incident unfolds over time. As such, we suggest that the SEC require periodic updates, possibly filed with ongoing quarterly and annual reporting. Such a procedure not only provides an accurate view of the situation but also fulfills all three roles of the SEC.

2.2 Designate certain large providers as systemically important cyber risk institutions

Rajgopal and Gezer (2018) suggest that Amazon Web Services (AWS) is clearly a systemic risk.[4] But we currently have no idea how many public (and private companies) are hooked into AWS, and what the cumulative dollar value of business interruption for companies reliant on AWS might be. A vulnerable API (application programming interface) from a relatively small startup company on AWS has the potential to bring down electronic commerce in a large part of our economy. One can extend this argument to several cloud providers such as Salesforce, Google and Microsoft and Apple. The SEC might want to consider more expansive disclosures of cyber risk of systemically important cyber institutions and enhanced enforcement of such disclosures.

We also suggest that these systemically important cyber institutions be subject to scenario-based testing to identify their ability to withstand and recover from cyber incidents and the outcomes of these tests be reported to investors. These tests would be the cyber equivalent of subjecting certain systemically important financial institutions to stress tests (i.e., Comprehensive Capital Analysis and Review (CCAR)). Such tests and reporting thereof may also lead to expansion of NGO efforts, such as Sheltered Harbor[5], into other sectors to promote operational resilience. We are aware of some efforts in this area but those are largely grass roots initiatives and often sector specific. Greater focus on disclosures of systemically important cyber institutions will cover all the three of the SEC's stated roles, especially related to the orderly functioning of markets and efficient capital allocation.

2.3 Require disclosures on the value of lost IP and data

---

[4] Gezer and Rajgopal. FORTUNE, October 4, 2018. Available at https://fortune.com/2018/10/04/facebook-data-breach-accounts-hacked/

[5] Sheltered Harbor, https://shelteredharbor.org/

We are concerned about the value of intellectual property that is being stolen by hackers from U.S. companies, especially at the behest of state actors. Requiring companies to measure and hence report the loss of intellectual property will shed more light on this pressing issue and potentially create investor pressure on companies to fortify their defenses or advocate more strongly with appropriate government agencies to stop or counter the loss of such IP.

The value of the lost IP and data needs to address not only the value to the entity but also to the capital markets and the economy. For example, several reports commissioned by the private sector and at least two branches of government (i.e., Legislative, Executive) have designated certain technologies and data key to our long-term viability as a nation: (i) the Cyberspace Solarium Commission[6]; (ii) the Economic Report of the President[7]; and by (iii) the Office of the Director of National Intelligence. In 2014, The U.S. Department of Commerce estimated that stolen IP cost the U.S. Economy between $200 billion and $250 billion annually.[8] This number has clearly grown in the recent past.

The U.S. Department of Defense (DoD) estimates an annual loss of approximately $57 billion from the theft of IP, which prompted them to create the Cybersecurity Maturity Model Certification (CMMC) and forced all defense contractors to comply if they want to continue in the defense business.

The disclosure must address how the lost IP and data affect the organization but also the larger economy. For example, we know artificial intelligence, the bio-economy, autonomous systems, quantum information science and technology, and semiconductors. are highly valued by our adversaries and threaten the U.S. presence on the global stage in the long term.[9]

The Marriott delayed disclosure mentioned earlier is an example of where the delayed reporting likely impacted others. Many believe the more significant impact of this particular Marriott breach is the credential harvesting and intelligence gathered by hackers to execute additional attacks. The delayed reporting prevented others from taking corrective action. Even if only the informal notice described in this letter were provided, others could have been notified and hence could have decided for themselves if corrective action was warranted.

2.4 Require disclosures on IT infrastructure and how its cyber hygiene is appropriate to protect its assets

Rajgopal and Gezer (2018) suggest that the SEC ask a company to clearly disclose the nature of its IT infrastructure.[10] For example, is the infrastructure located on the company's premises, or is it

---

[6] https://www.solarium.gov/home

[7] https://www.govinfo.gov/app/collection/erp/2019

[8] *Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank*, Com. Blog (Nov. 29, 2011), http://www.commerce.gov/blog/2011/11/29/stolen-intellectual- property-harms-american-businesses-says-acting-deputy-secretary-.

[9] https://www.dni.gov/index.php/ncsc-newsroom/item/2254-ncsc-fact-sheet-protecting-critical-and-emerging-u-s-technologies-from-foreign-threats

[10] Gezer and Rajgopal. Fortune, October 4, 2018. Available at https://fortune.com/2018/10/04/facebook-data-breach-accounts-hacked/

outsourced? And what is the dollar budget devoted to that infrastructure? The budget, as compared to the total revenue of a business, will give investors a sense for whether the firm under-invests in such infrastructure. Doing so also helps investors and other stakeholder understand the organizations reliance on technology and data.

We recommend disclosure on both hardware and software spending for the business, including data on personnel and training, and specific disclosure of the cybersecurity budget. If any material portion of the IT infrastructure is outsourced, the company should disclose the vendors and provide an outline of the services provided by such vendors. The idea is to be able to create comparable ratios in industries to identify companies that under-invest in this area. Disclosure on cybersecurity training is especially important, because 90% of cyberattacks exploit preventable human mistakes.

We recognize there is a balance between disclosing sufficient information to meet the SEC's three roles while not providing adversaries insights into how best to attack the enterprise. For example, the new rules propose disclosing an organization's policies and procedures. In practice, this is not practical because of the sheer volume of data and rate of change. It also has the deleterious effect of making the hackers job easier by providing deeper insight into the organization. A boilerplate disclosure is of no use to investors either. Hence, we see only downside to disclosing excessively detailed policies and procedures.

2.5 Require disclosures daily value of business interruption

If an automotive company produces 120,000 cars per year and the revenue per car is $10,000, the daily revenue lost by a cyberattack to its factory that relies heavily in robotics would be around $3.3 million. Skeptics might wonder whether revealing this would represent an open invitation to hackers to go after a company. We counter-argue that hackers are already aware of high-value targets. Better disclosures about, at least, the ranges of daily value of business interruption would reduce investors' estimation risk associated with evaluating the cash flow loss from an attack.

Historically, reports have largely focused on the value of assets including data. Over the years we have seen an exponential growth in attacks on availability. Ransomware is a prime example. Ransomware is effective because it prevents an organization from operating by denying access to its data. The total cost is a mix of loss of operations, cost of recovery, and reputational loss.

As we have seen with incidents at Colonial Pipeline and JBS (meat packing), these attacks can take a business offline and can result in a loss of revenue, expose the organization to liabilities, and erode its reputation. In 2016 the Justice Department unsealed indictments against individuals allegedly working on behalf of the Iranian government accused of carrying out distributed denial-of-service attacks against dozens of American banks as well as attempting to seize control of Bowman Dam outside New York City.[11]

Knowing the daily value of business interruption goes a long way towards fulfilling all of the SEC's three roles while enabling investors and stakeholders to make informed capital allocation decisions.

2.6 Require disclosures of continuity planning

A continuity plan identifies the critical information an organization needs to continue operating during an unplanned event, such as a cyberattack or natural disaster. The plan then highlights

[11] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

systems and processes that must be sustained and details how the company plans to keep these going. We request the SEC to consider asking for disclosures on continuity planning.

While we understand there may be reluctance to openly disclose the full plan because of the benefit to the adversaries, a set of basic metrics, common to the discipline can be disclosed. For example, the SEC might want to consider the following measures:

- Frequency and extent of Business Impact Assessments (BIA)[12]
- Recovery Time Objective (RTO)[13]
- Recovery Point Objective (RPO)[14]
- Service Delivery Option (SDO)[15]
- Maximum Tolerable Outage (MTO)[16].

In this increasingly connected world and the with the rise of incidents from third parties, the disclosure requirements should go one step further. At a minimum, the essence of an organization's Third-Party Risk Management (TPRM) program needs to be disclosed. Organizations who are required by others to meet their obligations must disclose such obligations (e.g., if an organization starts incurring fines as per its contract after being unavailable for four hours).

2.7 Board composition

The SEC rules ask about board composition. We absolutely believe it is important to disclose the cyber expertise of the board to meet the SEC's three stated roles. However, we believe, it is equally important to not require the expertise of particular individuals or their roles in cyber specific activities be disclosed. Making such disclosure voluntary is necessary to protect both the organization and promote access to board members of the highest quality. Disclosing specific expertise or roles of board members could make them and their families targets of nefarious activities such as extortion and doxing. Hence, the organization and/or the individuals may choose to make this level of disclosure, but it should not be mandated.

As usual, please feel free to contact us if you have any questions or would like to explore any of these points further.

Sincerely,

Shiva Rajgopal
Columbia Business School

Alex Sharpe
Sharpe Consulting LLC

[12] https://www.ready.gov/business-impact-analysis

[13] https://www.acronis.com/en-us/blog/posts/rto-rpo/

[14] https://www.acronis.com/en-us/blog/posts/rto-rpo/

[15] https://www.lawinsider.com/dictionary/service-delivery-objective-sdo

[16] https://csrc.nist.gov/glossary/term/maximum_tolerable_downtime