Seeking Closure On Disclosures

Russ Banham

FEATURED, SPECIAL REPORTS

Having long clamored for enhanced ESG transparency, investors are close to getting their wishes. In March, the Securities and Exchange Commission issued proposals for public companies to disclose their cybersecurity and climate change risks in financial statements. In the works is another SEC proposal involving the disclosure of human capital management policies and practices.

Assuming the three proposals reach a final stage of rulemaking with little change, they will add to a CFO's reporting obligations and related legal accountability. Under the CEO/CFO Certification Requirement of the Sarbanes-Oxley Act, CEOs and CFOs must personally certify the accuracy of a public company's financial statements.

"Like other CFOs I talk with regularly, no one is exactly sure how ESG will be monitored, other than it will be," said Mark Partin, CFO at publicly traded BlackLine, a provider of financial and accounting software and services, with $425.7 million in 2021 revenues and more than 1,800 employees globally.

Fortunately, finance chiefs like Partin and other strategic CFOs have amassed a skills set that would humble their forebears. Immersed in their organizations' fiscal health, technology underpinnings, customer experiences and enterprise operations, no other senior management leader has what it takes to oversee such rarefied disclosures.

Such is the case with the SEC's 129-page cybersecurity proposal (https://www.sec.gov/rules/proposed/2022/33-11038.pdf?mkt_tok=NDE3LUxYRi01NjUAAAGDMvek5yyT4g64xK1OzWFgCZqs4psUSfRAYKqq-TMryrzzRiAhHBMgpegX26fwZElvR2PRZHwpyY_mz7VeQHloTr2zQiYLMR3Zd3-RTWEt9A). Public companies would be required to report material cyber incidents within four business days, disclose their cybersecurity governance practices and expertise, and provide periodic updates of previously reported cyber incidents.

In a statement announcing the proposal, SEC Chair Gary Gensler called cybersecurity an "emerging risk…with significant financial, operational, legal and reputational impacts…Investors want to know more about how issuers are managing those growing risks."

It is understandable why shareholders would want this information. A startling number of successful ransomware attacks over the last two years resulted in records payouts and serious reputational damage for victim companies. According to the FBI's 2021 Internet Crime Report, cybercrime reported losses in 2021 were the highest in history, surpassing $6.9 billion, compared to an average of $2.95 billion in losses in the prior four years.

The figures represent a small fraction of total statistics, according to McKinsey & Co., citing FBI estimates suggesting that only 10 to 12 percent of cybercrimes ultimately are reported. "Investors want a clearer picture of a company's cybersecurity readiness," said Justin Greis, partner and leader of McKinsey's Cybersecurity, Digital and Technology practices. "The implication is `do we have confidence that a company can detect and triage cyber incidents in its environment,' something that a lot of organizations struggle with today."

For investors to acquire this confidence, the SEC seeks to impose an obligation on public companies to report material cyber incidents and related pre-incident security and post-incident response processes. This obligation creates liability for CFOs, CEOs and board directors, said Dan Bailey, partner at the Columbus, Ohio-based law firm Bailey Cavalieri, which often represents insurer defendants in director and officer liability litigation. "The government figures it has a better chance of influencing corporate behavior by getting the board and key executives like the CFO to focus on investor disclosures, which is their biggest liability," he explained.

Putting aside such liability, public company CFOs like Partin at BlackLine have been engaged for some time in preparing for the inevitability of ESG disclosures. “I think it would be naïve to think that nothing needs to change to capture the increased SEC reporting requirements,” said Partin. “Great companies are those that lean forward to the maximum extent as possible, getting in front of where things are headed even if they don’t come to pass.”

Other CFOs share this perspective. “We’re doing everything we can to stay in front of this,” said Richard Galanti, CFO at retail giant Costco, with $195.9 billion in 2021 revenue. “We’re setting up systems to collect the related data as quickly as it is produced and making sure it is auditable.”

Material Downsides

During the public comment period on the SEC’s Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposal, many comments pertained to the difficulties in determining a cyber incident’s materiality within four business days of its discovery. As PwC wrote, “completing a materiality determination could take several weeks to months from initial identification of an incident, depending on its complexity.”

The audit and advisory firm stated that it supported disclosing a material cyber incident “as soon as reasonably practicable,” as opposed to four business days.

McKinsey’s Greis agreed that determining the materiality of cyber incidents is a complicated and time-consuming decision, due in no small part to the fact that many IT networks are bombarded with hundreds of cyberattacks on a weekly basis. “Cyber is a bit tough to course out when it comes to materiality,” he said.

“If a hacker gains access to a company’s customer list and puts it on the Dark Web, that’s clearly a material impact,” he said. “On the other hand, say there is evidence that a hacker has gained access to the network and is doing network reconnaissance and enumeration but hasn’t actually exfiltrated any data. That’s important information to the company, but whether it’s material for reporting purposes isn’t clearly defined. It’s a question mark.” Network surveillance and enumeration involves the gathering of information by rogue actors about a target network.

Other gray areas in the cybersecurity proposal involve the disclosure of procedures used to identify and manage cybersecurity risks. The challenge in providing this information is how much to provide. If registrants under-report their cybersecurity risks and suffer a major cyberattack, this could be ammunition for a successful plaintiff lawsuit. If companies over-report their risks, they could expose a potential cybersecurity weakness. “It’s a fine line to walk, but the SEC’s intent is to encourage companies to drive the right behaviors to continually improve their cybersecurity,” Partin said.

Leading the ESG Team

Given that there are soon to be three ESG-related disclosure proposals requiring public company obligations, now is the time for CFOs to ensure proper processes are in place to gather accurate data for reporting purposes.

“As the new cybersecurity and other disclosures come to pass, the CFO is looked to as the architect to make sure all the pieces are in place to report these risks,” said Todd Musgrove, director, Strategy and Business Transformation, at advisory firm The Hackett Group. “Their knowledge of the business, operations and customers gives CFOs the best perspective to determine which cyber incidents are material for reporting purposes.”

He is not alone in this view. “The best CFOs act as the translation layer between the technical things that happen in the environment and the impact of these events on the business,” said Greis from McKinsey. “They have an operational view of what is happening on the ground and are able to listen, understand and translate what it all means.”

Both Galanti and Partin fit this profile. “We take things like cybersecurity, climate change, ESG and DE&I very seriously here,” said Galanti. “My role is to make sure we’re fulfilling these needs in a correct and timely fashion, putting in place the proper people, controls and technologies to do what is required.”

Moving forward, Musgrove said it is “incumbent upon CFOs to make sure the right team is in place to keep track of the SEC requirements as they evolve. As the architect, the CFO needs to set up the governance structure to proactively prepare for these eventual reporting obligations.”

The “right teams” are cross-functional, composed of internal subject matter experts in cybersecurity, climate risks and human capital management practices, and in-house legal counsel and compliance professionals, he said. Each team should be co-chaired by the CFO with the respective function leader, such as the CISO for the cybersecurity disclosure committee.

McKinsey is recommending as an emerging best practice to its clients that the board and senior management establish a cybersecurity committee and team, respectively, to address the future reporting requirements. “Generally, boards have relied on the audit committee to oversee cyber, but we’re beginning to see separate standalone cyber committees and cyber subcommittees of the audit committee, especially following a massive cyberattack,” Greis said.

The CFO should play a leadership role in these committees and teams. “They not only have an operational view to bring to the table, they’re also instrumental when it comes to post-attack restoration,” Greis said.

“The best CFOs I’ve seen in this crisis situation know which system to bring up first, second and so on, a decision based on the dependencies of the business,” he explained. “Otherwise, the IT security team will bring them up in the order they view as expedient, which may not be in the best interest of the business.”

Greis noted that some McKinsey clients have found value in sourcing advice from third-party panels composed of experienced CISOs. “The idea here is to have the panel pressure-test the company’s cybersecurity strategy and plans on a quarterly or biannual basis, which is a means towards obtaining valuable and constructive feedback,” Greis said.

Partin touts the value of close collaborations between CFOs and CISOs. “As every company automates business and work processes, digitalizes its data and invests in cloud solutions, it is incumbent upon the CFO to work closely with CISOs and outside tech security vendors to understand the risks and what is being done about them,” he said.

Private Matters

Not just public company CFOs are closely watching the progress of the SEC’s cybersecurity and other ESG-related disclosure proposals. “We’re being asked by our owners, investors and lenders to fill out ESG checklists, (which is) a form of disclosure,” said Steve Horowitz, CFO at privately held CareCentrix, a provider of post-acute care management to 20 million members, with about $1.5 billion and 1,800 employees throughout the U.S.

Horowitz said he struggles with the rationale behind the SEC’s proposed reporting requirements, which seems redundant. “The SEC already requires companies to report any risks that are material,” he explained. “All that information is in the 10-K. If an ESG-related risk is material, it should be in what is reported. It seems like the SEC is looking to be politically correct instead of its stated purpose to protect investors. The disclosures could become a distraction from generating value for shareholders.”

Regarding the cybersecurity risk disclosures, he said that most public companies and even those that are privately held have developed response plans in the event of a cyber incident.

“Hopefully every business is prepared and has an idea what to do to limit the damage,” said Horowitz. “I don’t think anyone is looking to sweep this under the rug. But it’s an awful lot to be coordinating and then have to simultaneously report the incident to regulators in four business days. It takes time to process these things.”

For the time being, CFOs eagerly await the SEC’s definitive rulemaking. As Partin put it, “Something will come out of all this, but what the final disclosures will look like is still very much open to debate. Nevertheless, if you aren’t getting out ahead of these potential regulatory requirements being worked through the system over the next three to five years, you’ll have some significant catchup to do that may impact the sustainable growth of your business.”

Russ Banham

Russ Banham is a Pulitzer-nominated business journalist and best-selling author.