LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Getting Ahead Of The SEC's Continued Focus On Cyber, AI

By **Carolyn Welshhans and Kelly Gibson** (May 2, 2025, 1:22 PM EDT)


Carolyn Welshhans


Kelly Gibson

Since the change in administration, the U.S. Securities and Exchange Commission has received a lot of attention for what it is not going to do going forward, including dismissals of a number of crypto-related lawsuits. But it is just as important to consider where the SEC is likely to focus its time and resources, and to prepare accordingly.

Two such areas are cybersecurity and artificial intelligence, where the SEC has been putting down markers that it is going to continue to scrutinize the actions of public companies and regulated entities such as investment advisers and broker-dealers.

Companies and financial institutions should consider how the SEC's recent actions in these spaces affect their businesses. By doing so, they can use these lessons to take proactive measures to avoid regulatory scrutiny going forward.

The SEC's emphasis on cybersecurity and AI is likely unavoidable, given the prevalence of these two topics and their impact on all of us. In 2023, the FBI's Internet Crime Complaint Center reported 880,418 complaints filed by Americans for cyber-related issues, with a loss of $12.5 billion.[1]

These were record figures and reflected an increase of 22% in losses by Americans over the prior year; however, these numbers only reflect incidents Americans choose to report, not the many others that go unreported. One industry trade group estimates that global cybercrime costs will reach $10.5 trillion in 2025.[2] No sector of the economy is immune, with nearly one-fifth of all incidents affecting financial firms.[3]

Meanwhile, AI's growth continues to explode. For example, one estimate places the global market for AI-related services and products at as much as $900 billion by 2027, with an annual growth of 40-55% over the next several years.[4] As the SEC under new leadership looks for issues that affect retail investors, cybersecurity and AI will fit that bill.

What lessons can we learn from the SEC's cybersecurity and AI activity thus far?

Over the last several years, the SEC has been active in cybersecurity and AI matters across its divisions and offices. And just last month, on March 27, it held a roundtable focused on AI.[5]

It remains to be seen what, if any, rulemaking for cybersecurity and AI the SEC will take up under the

new leadership. With respect to enforcement proceedings, however, the message since the change in administration has been clear: The SEC is continuing to focus on and devote resources to these issues.[6]

For example, in February, the SEC announced the creation of the Cyber and Emerging Technologies Unit in the Division of Enforcement, replacing the former Crypto Assets and Cyber Unit.[7] The CETU's stated priorities include combating, among other things, hacking to obtain material nonpublic information, regulated entities' compliance with cybersecurity rules and regulations, and public issuer fraudulent disclosure relating to cybersecurity, as well as fraud committed using AI.[8]

Those familiar with SEC practice will note that these stated priorities are consistent with the stated priorities of the original Cyber Unit that was formed in 2017 under Chair Jay Clayton during President Donald Trump's first term.[9]

To that end, the SEC continues to highlight recent enforcement actions in this space,[10] including actions filed against those who offered investment opportunities with false statements regarding AI capabilities. And while we have yet to see an enforcement action against a public company under the new rules for cybersecurity disclosures, it is clear based on the CETU's stated priorities that the SEC will continue to focus on materially false or misleading statements by companies relating to cyber breaches, albeit returning to a reliance on traditional theories of materiality[11] instead of on aggressive theories relating to internal controls or disclosure controls violations.

So, what can we expect going forward?

First, we should expect some increasingly sophisticated cases. To date, the SEC has filed actions involving some low-hanging fruit concerning AI, focused on investment advisers and companies that claimed to be using AI when they allegedly were not. These were relatively simple fraud cases that emphasized the alleged failures of companies and individuals to do what they promised.

In addition to these cases, we expect the SEC to broaden its scope to include fraud cases in which the AI matches some, but not all, of the disclosures. We also expect that the SEC may take on risk disclosures, particularly if public companies suffer large losses as a result of their AI use or AI used against them.

Second, as signaled in the SEC's announcement of the CETU, the SEC is poised to look more closely at whether the policies and procedures of financial institutions are addressing cybersecurity risks.

The SEC has brought cases in this area, including for violations of Regulations SCI, S-P and S-ID, which are aimed at covered financial institutions addressing the risks of cybersecurity incidents. Most of these cases have not been viewed as controversial or partisan within the SEC.

If the deficiencies at financial institutions are perceived to be serious enough and the potential harm to customers — particularly retail investors — is great enough, we expect to see additional enforcement cases even without a fraud component. We similarly may see the SEC expand and use these and other policy and procedure provisions to address financial institutions' approaches to AI.

Third, we expect to see the SEC lean into its use of data, both in terms of sourcing cases and in investigating these matters. These efforts have included the sophisticated analysis of trading data, scraping of public company filings, scrutiny of voluminous financial data, examination of social media posts and more.

For example, SEC enforcement proceedings in the cybersecurity area have already relied on the Division of Enforcement's use of forensic evidence, with public references to very technical details of how threat actors compromised and maneuvered through companies' systems, including citations to logs, and the tracing and linking of IP addresses, servers and other artifacts.

We expect this work to continue in cybersecurity investigations, and we also expect the SEC to focus more on trading data to determine if any insider trading occurred around companies' discovery of cybersecurity incidents.

The SEC has also announced that the CETU will focus on the use of social media, the dark web and false websites to perpetrate fraud. In its press releases announcing AI cases, the SEC has linked to an investor alert that warns about the use of AI-enabled deepfake videos and audio to spread false or misleading information.

If a market event appears to result from AI-related activity, such as through the use of a deepfake or due to an AI trading program's hallucination, the SEC would likely follow its playbook for cases involving runaway trading algorithms and other order placement issues, with a heavy emphasis on trading data, algorithmic inputs, specifics of software code and reconstruction of voluminous order books.

Finally, public companies and financial institutions should not be surprised by parallel investigations that involve the SEC and other regulators and members of law enforcement. The SEC frequently works in tandem with the U.S. Department of Justice and the FBI, typically with units that focus on financial and securities fraud.

Cybersecurity issues bring in less regular players, such as the DOJ's National Security Division and the U.S. Department of the Treasury, including its Office of Foreign Assets Control. AI investigations may overlap with cybersecurity matters, and both areas have seen increasing interest from state attorneys general and international regulators.

With all of this activity, what takeaways should companies and firms keep front of mind?

Many entities are already focused on cybersecurity because of its significant impact on business operations. Likewise, many companies and financial institutions are working through how AI may enhance efficiencies, customer interactions, back-office operations and more. As companies and firms grapple with these considerations, they should ensure that their cyber and AI hygiene addresses issues of concern to the SEC.

In particular, it is important to review and update policies and procedures for handling cybersecurity incidents and risks posed by AI, with the latest SEC regulations and enforcement proceedings taken into account. Similarly, public companies and financial institutions should make sure that their incident response plans include the escalation of key information to decision-makers with the responsibility of determining disclosures to the SEC, investors and customers, as appropriate.

The SEC rules do not impose a one-size-fits-all standard, which means that companies and financial institutions should tailor their policies and procedures for risks specific to their business model, customers and operations.

If a cybersecurity or AI-related event does occur, the SEC's primary focus will be on whether disclosures to investors or customers were required, and, if so, whether they were materially false or misleading.

Deciding whether such an event necessitates disclosure, especially in an environment where cybersecurity incidents happen so frequently, requires careful consideration.

Public companies and financial institutions will need to determine not only whether to make affirmative disclosures, but also whether the event in question has implications for prior disclosures. It is a good practice to periodically consider whether any disclosures should be updated in light of changes to an entity's risk profile, experiences or other factors.

Companies and firms should also have a handle on what data they possess, in what form, and any preservation requirements their policies and procedures currently impose. Again, many entities already take these issues into consideration for business reasons, such as the need to reconstruct trading events or as part of their cybersecurity protection measures. But regulators may express interest in logs and other forensic data.

Similarly, public companies and financial institutions should understand how their interactions with vendors or other third parties may implicate their cybersecurity and/or AI risk profile. For example, entities should understand how any vendors are protecting their data or their customers' data, and conduct due diligence early and periodically when sensitive information is handled by third parties.

Cybersecurity is an issue permanently entrenched in our financial markets, and AI is rapidly reaching to join it. In a global market system, these two issues have a widespread impact and the potential for significant repercussions.

It therefore is not a surprise that the SEC is so focused on cybersecurity and AI, even with the change in administration. As a result, public companies and financial institutions should consider their regulatory risks when it comes to cybersecurity and AI, and work to reasonably address the implications for their particular business on an ongoing basis.

Carolyn Welshhans is a partner at Morgan Lewis & Bockius LLP. She previously held a number of leadership roles at the SEC, including associate director and acting data officer of the Division of Enforcement, as well as assistant director in the Enforcement Division's Cyber and Market Abuse units.

Kelly Gibson is a partner and co-leader of the securities enforcement practice and the ESG and sustainability advisory practice at Morgan Lewis. She previously held numerous leadership roles at the SEC, including acting deputy director of the Division of Enforcement, leader of the Enforcement Division's Climate and ESG Task Force, and director of the SEC's Philadelphia Regional Office.

[1] https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.

[2] https://www.cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[3] https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024.

[4] https://www.bain.com/about/media-center/press-releases/2024/market-for-ai-products-and-services-could-reach-up-to--$990-billion-by-2027-finds-bain--companys-5th-annual-global-technology-report/.

[5] https://www.sec.gov/newsroom/press-releases/2025-56.

[6] https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-iac-030625.

[7] https://www.sec.gov/newsroom/press-releases/2025-42.

[8] https://www.sec.gov/newsroom/press-releases/2025-42.

[9] https://www.sec.gov/newsroom/press-releases/2017-176.

[10] https://www.sec.gov/newsroom/speeches-statements/uyeda-remarks-enforcement-directors-panel-022025.

[11] https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-northwestern-securities-regulation-institute-012725.