STATEMENT

Statement Regarding Administrative Proceedings Against SolarWinds Customers

Commissioner Hester M. Peirce (/about/sec-commissioners/hester-m-peirce)

Commissioner Mark T. Uyeda (/about/sec-commissioners/mark-t-uyeda)

Oct. 22, 2024

According to the Government Accountability Office, the 2019-2020 cyberattacks against SolarWinds Corporation ("SolarWinds") and its Orion software were "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and the private sector."[1] It was an attack against America.[2] How has the Commission responded? By first charging SolarWinds in district court[3] and, in today's settled proceedings,[4] charging four customers of its Orion software, with violations of the federal securities laws. Today's proceedings impose nearly $7 million in penalties against these victims of the cyberattacks.

The four proceedings can be divided into two categories. Two of the companies – Avaya Holdings Corp. ("Avaya") and Mimecast Limited ("Mimecast") – disclosed information about the cyberattack.[5] However, the Commission finds that the disclosures omitted certain material information.[6] The other two companies – Check Point Software Technologies Ltd. ("Check Point") and Unisys Corporation ("Unisys") – did not update an existing risk factor in response to the cyberattack.[7] The Commission finds that those risk factors became materially misleading without disclosure that the Orion software in the companies' respective network had been compromised.[8]

The common theme across the four proceedings is the Commission playing Monday morning quarterback. Rather than focusing on whether the companies' disclosure provided material information to investors, the Commission engages in a hindsight review to second-guess the disclosure and cites immaterial, undisclosed details to support its charges. Accordingly, we dissent.

Avaya and Mimecast

Avaya

With respect to Avaya, the Commission highlights "the likely attribution of the [cyberattack] to a nation-state threat actor" as an example of omitted material information.[9] The Commission's view that such information is material is troubling for a couple of reasons.

First, in its 2023 rulemaking on cybersecurity incident disclosure (the "2023 Cybersecurity Rule"),[10] neither investors nor the Commission expressed a view that the identity of the threat actor is material information. When proposing the 2023 Cybersecurity Rule, the Commission sought public feedback on whether there were specific types of information that should be disclosed for a material cybersecurity incident.[11] Not a single one of the 150-plus comment letters submitted on the proposal requested disclosure of the identity of the threat actor.[12] Accordingly, it is highly unlikely that investors consider this information to be material. When adopting the 2023 Cybersecurity Rule, the Commission stated that disclosure of cybersecurity incidents should "focus…primarily on the impacts of…[the]…incident, rather than on…details regarding the incident itself."[13] The identity of the threat actor, while an obvious "detail…regarding the incident," lacks a clear link to the "impact" of the incident. By using a settled proceeding to convey the view that this information is material, the Commission regulates by enforcement.

Second, by the time Avaya disclosed information about the cyberattack in February 2021, there had already been widespread media reports[14] and a joint statement by government agencies[15] that Russia was the likely threat actor. Although Avaya's disclosure did not tie its incident to the SolarWinds cyberattack, it is unlikely that attribution of the incident to Russia would have "significantly altered the 'total mix' of information"[16] about Avaya to a reasonable investor in light of the existing public information about the cyberattack.

The Commission's other factors for why Avaya omitted material information are equally unconvincing. The Commission cites "the long-term unmonitored presence of the threat actor in Avaya's systems, the access to at least 145 shared files some of which contained confidential and/or proprietary information, and the fact that the mailbox the threat actor accessed belong to one of Avaya's cybersecurity personnel."[17] These are the "details regarding the incident itself" – as opposed to the "impact" of incident – that the Commission has said do not need to be disclosed.[18]

Mimecast

Although the Form 8-K requirements for disclosing material cybersecurity incidents, which were adopted as part of the 2023 Cybersecurity Rule, did not yet apply to Mimecast, it filed three Form 8-Ks related to the intrusion of the Orion software on its network.[19] In the third Form 8-K, Mimecast filed its three-page incident report for the cyberattack as an exhibit.[20] Mimecast's efforts to inform its investors would not be rewarded; the Commission finds fault with its disclosures, particularly regarding "the large number of impacted customers and the percentage of code exfiltrated by the threat actor."[21]

The Commission highlights Mimecast's failure to disclose that "the threat actor had accessed a database containing encrypted credentials for approximately 31,000 [of 40,000] customers."[22] Where the compromised information consists of a large percentage of customer credentials, disclosure of such fact *can be* material. In assessing materiality in the Commission's case against SolarWinds, the court stated that "perspective and context are critical" to evaluating whether a Form 8-K is materially misleading and that a filing is not misleading if "[the] disclosure, read as a whole, captured the big picture."[23]

Mimecast disclosed, without providing a percentage or number, that encrypted customer credentials had been accessed.[24] It said that the company was "resetting the affected… credentials."[25] Mimecast further disclosed that it found "no evidence that the threat actor accessed email or archive content held by [it] on behalf of [its] customers."[26]

In bringing charges against Mimecast, the Commission focuses on the detail of the threat actor accessing a database containing customer credentials, as opposed to the larger picture of the effects of the incident. Access to credentials, by itself, may not be material if the threat actor does not use the credentials to misappropriate customer information. Mimecast's disclosure, read as a whole, conveys the complete story about the unauthorized access of credentials and the lack of misappropriated information.

With respect to disclosure of exfiltrated source code, Mimecast stated in its incident report that the threat actor had downloaded a "limited number" of its source code repositories but the company believed that the downloaded code was "incomplete and would be insufficient to build and run any aspect of the Mimecast service."[27] The Commission finds that these statements were materially misleading because Mimecast did not disclose that the threat actor had exfiltrated "58% of its exgestion source code, 50% of its M365 authentication source code, and 76% of its M365 interoperability source code, representing the majority of the source code for those three areas."[28]

By calling for disclosure of specific percentages and types of source code, the Commission ignores the *reasonable* investor standard embedded within the materiality concept and the types of information that such investor would consider important in making an investment decision. We are doubtful that a reasonable investor would understand how exfiltration of

such precise percentages of those three types of source code affects Mimecast. Similar to the Avaya case, such information is "details regarding the incident itself"[29] that do not need to be disclosed. For us, the material disclosure by Mimecast is that the cyberattack did not result in modifications of the company's source code or have effects on its products.[30] Notably, the Commission did not find that such statement was materially misleading.

Effect on Form 8-K, Item 1.05 Disclosure

In addition to our concerns about the charges against Avaya and Mimecast, we are also concerned about how the proceedings against them will shape disclosure provided pursuant to new Item 1.05 of Form 8-K, which was adopted as part of the 2023 Cybersecurity Rule. This item requires companies to disclose "the material aspects of the nature, scope, and timing" of a material cybersecurity incident.[31]

Companies reviewing today's proceedings[32] reasonably could conclude that the Commission will evaluate their Item 1.05 disclosure with a hunger for details that runs contrary to statements in the adopting release.[33] To avoid being second-guessed by the Commission, companies may fill their Item 1.05 disclosures with immaterial details about an incident, or worse, provide disclosure under the item about immaterial incidents. The Commission staff has already identified the latter practice as an issue,[34] and today's proceedings may exacerbate the problem. As the Commission recognized when adopting the 2023 Cybersecurity Rule, immaterial disclosure about cybersecurity incidents may "divert investor attention" and result in "mispricing of securities."[35] However, if the Commission's enforcement actions have the practical effect of requiring immaterial disclosure, then the benefits and underlying rationale used to support the 2023 Cybersecurity Rule may be undermined.

Check Point and Unisys

The Commission's proceedings against Check Point and Unisys both rest on a similar theory: the company failed to update its cybersecurity risk factor for the Orion software compromise and left its risk factor generic (in the case of Check Point)[36] or as a hypothetical (in the case of Unisys).[37]

Check Point

In the SolarWinds case, the Commission argued that the SolarWinds risk factor was "unacceptably boilerplate and generic" because of "the company's internal recognition that its security systems were faulty."[38] The court rejected the argument after a detailed review of SolarWinds' risk disclosure and concluded that "[v]iewed in totality, [such] disclosure was sufficient to alert the investing public of the types and nature of cybersecurity risks SolarWinds faced and the grave consequences these could present for the company's financial health and future."[39]

In its proceeding against Check Point, the Commission argues that the company's risk disclosure was generic and should have been revised because its cybersecurity risk profile had materially changed.[40] This contention, however, merits cautious consideration in light of the SolarWinds court's reasoning in dismissing portions of the Commission's case against SolarWinds, which, as illustrated below, was based on arguably similar disclosures.

Court's reason for why SolarWinds risk disclosure was not generic[41]	**SolarWinds risk factor, as quoted by the court[42]**	**Check Point risk factor[43]**
Disclosed specific risks the company faced given its business model	[SolarWinds was] vulnerable to damage or interruption from… traditional computer "hackers," malicious code (such as viruses and worms)…denial-of-service attacks[, and] sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions).	We or our products are a frequent target of computer hackers and organizations that intend to sabotage, take control of, or otherwise corrupt our manufacturing or other processes and products. We are also a target of malicious attackers who attempt to gain access to our network or data centers or those of our customers or end users; steal proprietary information related to our business, products, employees, and customers; or interrupt our systems or those of our customers or others.

Warned about the increasing frequency of attacks	The risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has generally increased the number, intensity and sophistication of attempted attacks.	We believe such attempts are increasing in number.
Warned that the company might prove unable to anticipate, prevent, or detect attacks	Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.	While we seek to detect and investigate all unauthorized attempts and attacks against our network and products, and to prevent their recurrence where practicable through changes to our internal processes and tools and/or changes or patches to our products, we remain potentially vulnerable to additional known or unknown threats.

Alerted investors to the potential for a security breach to have very damaging consequences to the company	The foregoing security problems could result in, among other consequences, damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information. The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.	Such incidents, whether successful or unsuccessful, could result in our incurring significant costs related to, for example, rebuilding internal systems, reduced inventory value, providing modifications to our products and services, defending against litigation, responding to regulatory inquiries or actions, paying damages, or taking other remedial steps with respect to third parties. Publicity about vulnerabilities and attempted or successful incursions could damage our reputation with customers or users and reduce demand for our products and services.

Unisys

The Commission's case against Unisys[44] rests on the finding that Unisys's risk factor framed cybersecurity events as hypothetical, even though a compromise of the Orion software on the company's network already had occurred.[45]

Risk factors are designed to warn investors about events that *could* occur and materially affect the company. To the extent that an event *has* occurred and *has* materially affected the company, it is generally required to be disclosed in another part of a filing, such as the description of the business, management's discussion and analysis, or the financial statements and notes thereto. Whether risk factors need to be updated because certain hypothetical risks have materialized is not always a straightforward matter,[46] and the Commission should be judicious in bringing charges in this area. If the Commission does not exercise restraint, it could find a violation in every company's risk disclosure because risk factors cover a wide range of topics and are inherently disclosure of hypothetical events. Aggressive enforcement by the Commission may cause companies to fill their risk disclosures with occurrences of immaterial events, for fear of being second-guessed by the Commission. Such a result would frustrate the Commission's goal of preventing a lengthy risk factor section filled with immaterial disclosure.[47]

In light of these considerations, the case against Unisys is one that did not need to be brought. The Commission advances three reasons for why the company's cybersecurity risk profile changed materially and its risk factor should have been updated.[48]

First, the Commission states that a "persistent and reportedly nation-state supported threat actor compromised the company's environment."[49] This factor does not show materiality because it merely says that a cybersecurity incident occurred, and not every incident is material.

Second, the Commission finds that "the threat actor persisted in the environment unmonitored for a combined span of at least sixteen months."[50] While this fact is concerning from an information security perspective, the Commission fails to elaborate on why it is material from a securities law perspective. Notably, the Commission did not find that Unisys's financial results were adversely affected or its reputation had measurably declined, especially relative to its peers given the widespread nature of the SolarWinds cyberattack.

Finally, the Commission says that "[Unisys]'s investigation of the activity suffered from gaps that prevented it from identifying the full scope of the compromise."[51] It is unclear to us how an after-the-fact investigation of a cybersecurity incident affects the materiality of the incident itself. The Commission did not find that the unidentified aspect of the compromise materially affected Unisys. Similar to the second reason, the Commission fails to explain how a subpar investigation relates to adverse effects on the company.

Because we are not persuaded by the Commission's arguments on the materiality of Unisys's cybersecurity incident, we do not support the charges against the company.

Conclusion

Cybersecurity incidents are one of a myriad of issues that most companies face. The Commission needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one. Yes, the Commission must protect investors by ensuring that companies disclose material incidents, but donning a Monday morning quarterback's jersey to insist that immaterial information be disclosed — as the Commission did in today's four proceedings — does not protect investors. It does the opposite.

---

[1] SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response, WatchBlog (Apr. 22, 2021), available at https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic).

[2] *See, e.g.*, A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack, Dina Temple-Raston, NPR All Things Considered (Apr. 16, 2021) ("Hackers…used [a] routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America."), available at https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack).

[3] The court recently dismissed most of the claims the Commission brought against SolarWinds. *SEC v. SolarWinds Corp.*, 2024 WL 3461952 (S.D.N.Y. July 18, 2024).

[4] In the Matter of Avaya Holdings Corp., Release No. 34-101398 (Oct. 22, 2024) ("Avaya Order"), available at https://www.sec.gov/files/litigation/admin/2024/33-11320.pdf (https://www.sec.gov/files/litigation/admin/2024/33-11320.pdf); In the Matter of Check Point Software Technologies Ltd., Release No. 34-101399 (Oct. 22, 2024) ("Check Point Order"), available at https://www.sec.gov/files/litigation/admin/2024/33-11321.pdf (https://www.sec.gov/files/litigation/admin/2024/33-11321.pdf); In the Matter of Mimecast Limited, Release No. 34-101400 (Oct. 22, 2024) ("Mimecast Order"), available at https://www.sec.gov/files/litigation/admin/2024/33-11322.pdf (https://www.sec.gov/files/litigation/admin/2024/33-11322.pdf); and In the Matter of Unisys Corporation, Release No. 34-101401 (Oct. 22, 2024) ("Unisys Order"), available at https://www.sec.gov/files/litigation/admin/2024/33-11323.pdf (https://www.sec.gov/files/litigation/admin/2024/33-11323.pdf).

[5] Avaya Order at paragraph 10 and Mimecast Order at paragraphs 9-13 and 15-16.

[6] Avaya Order at paragraph 10 and Mimecast Order at paragraphs 9, 14, and 16-17.

[7] Check Point Order at paragraph 13 and Unisys Order at paragraph 19.

[8] Check Point Order at paragraphs 15-16 and Unisys Order at paragraph 19.

[9] Avaya Order at paragraph 10.

[10] While the facts of the proceedings against Avaya and the other three companies predate the 2023 Cybersecurity Rule, the new requirements inform our analysis of, and dissent on, these proceedings.

[11] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038 (Mar. 9, 2022) [87 FR 16590, 16597 (Mar. 23, 2022)] ("Is there any additional information about a material cybersecurity incident that…should [be] require[d]?"), available at https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure (https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure).

[12] Comment letters submitted on the 2023 Cybersecurity Rule are available at https://www.sec.gov/comments/s7-09-22/s70922.htm (https://www.sec.gov/comments/s7-09-22/s70922.htm).

[13] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023) [88 FR 51896, 51903 (Aug. 4, 2023)] ("2023 Cybersecurity Adopting Release"), available at https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure (https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure).

[14] *See, e.g.*, Suspected Russian Hack is Much Worse than First Feared: Here's What You Need to Know, Sam Shead (Dec. 19, 2020), available at https://www.cnbc.com/2020/12/18/suspected-russian-hack-on-us-is-much-worse-than-first-feared.html (https://www.cnbc.com/2020/12/18/suspected-russian-hack-on-us-is-much-worse-than-first-feared.html).

[15] *See* U.S. Feds Say Russians Likely Behind SolarWinds Hack that Breached Government Networks, Todd Haselton (Jan. 5, 2021), available at https://www.cnbc.com/2021/01/05/us-feds-say-russians-likely-behind-solarwinds-hack.html (https://www.cnbc.com/2021/01/05/us-feds-say-russians-likely-behind-solarwinds-hack.html).

[16] *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976).

[17] Avaya Order at paragraph 10. The Commission also takes issue with Avaya's disclosure that there was "no current evidence" of access to its "other internal systems." *Id*. The Commission acknowledges that the statement was facially accurate but finds that it was made misleading because Avaya did not disclose the threat actor's access to 145 shared files in an external cloud environment. *Id*. For the same reason that we do not believe that disclosure about 145 files being accessed is material, we also do not believe that Avaya's statement about its internal systems is materially misleading.

[18] Note 13, *supra*.

[19] Mimecast Order at paragraphs 10-13.

[20] Exhibit 99.2 of Form 8-K filed on March 16, 2021 by Mimecast (the "Mimecast Incident Report"), available at https://www.sec.gov/Archives/edgar/data/1644675/000119312521082200/d141664dex992.htm (https://www.sec.gov/Archives/edgar/data/1644675/000119312521082200/d141664dex992.htm).

[21] Mimecast Order at paragraphs 9, 14, and 16.

[22] Mimecast Order at paragraphs 6 and 14. The Commission also finds that Mimecast's disclosure was materially misleading because it failed to disclose that the threat actor accessed server and configuration information for approximately 17,000 customers. Mimecast Order at paragraph 14. Mimecast disclosed in its incident report that the threat actor accessed server information. Mimecast Incident Report at p.1 ("[T]he threat actor accessed certain Mimecast-issued certificates and related customer server connection information."). The Commission fails to explain why the specific number of customers whose server and configuration information was accessed is material when the company had already disclosed that server information was accessed.

[23] *SolarWinds Corp.*, *supra* note 3, at 44, 46.

[24] Mimecast Incident Report at p.1 ("The threat actor also accessed a subset of email addresses and other contact information, as well as encrypted and/or hashed and salted credentials.").

[25] *Id*.

[26] *Id*.

[27] *Id.* at p.2.

[28] Mimecast Order at paragraph 16.

[29] Note 13, *supra*.

[30] Mimecast Incident Report at p.1 ("[W]e found no evidence of any modifications to our source code nor do we believe there was any impact on our products.").

[31] Item 1.05(a) of Form 8-K.

[32] Although the charges against Avaya stem from the company's risk factor disclosure, at issue is disclosure about a cybersecurity incident and so these charges may inform how companies provide disclosure under Item 1.05.

[33] *See* note 13, *supra*, and accompanying text.

[34] *See, e.g.*, Disclosure of Cybersecurity Incidents Determined to be Material and Other Cybersecurity Incidents, Erik Gerding (May 21, 2024), available at https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024 (https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024).

[35] 2023 Cybersecurity Adopting Release at 51929 ("Item 1.05 is thus expected to elicit more pertinent information to aid investor decision-making. Additionally, the materiality requirement should minimize immaterial incident disclosure that might divert investor attention, which should reduce mispricing of securities.").

[36] Check Point Order at paragraphs 13 and 15-16.

[37] Unisys Order at paragraph 19.

[38] *SolarWinds Corp.*, *supra* note 3, at 35.

[39] *Id*. at 35-36. The court also expressed the view that cautionary language, such as risk factors, do not need to be "articulated with maximum specificity" and that doing so "may backfire." *Id.* at 36. Additionally, the SolarWinds court dismissed the Commission's charges against SolarWinds for not updating its allegedly hypothetical risk factor for incidents that had materialized. *Id*. at 37-39.

[40] Check Point Order at paragraphs 12-13 and 15-16.

[41] *SolarWinds Corp.*, *supra* note 3, at 35.

[42] *Id*.

[43] Form 20-F filed April 2, 2021 at p.16, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1015922/000119312521104893/d112235d20f.htm (https://www.sec.gov/ix?doc=/Archives/edgar/data/1015922/000119312521104893/d112235d20f.htm).

[44] In addition to fraud and reporting violations, the Commission also finds that Unisys did not maintain disclosure controls and procedures, in violation of rule 13a-15(a) under the Securities Exchange Act of 1934. Unisys Order at paragraphs 26 and 31. While we disagree with that finding, we do not address the issue in this statement. However, we note that in discussing Unisys's cooperation, the Commission states that "Unisys took certain steps to remediate its control deficiencies, including…augmenting its cybersecurity personnel and

tools, both internally and externally, to strengthen its cybersecurity risk management and protections." Unisys Order at paragraph 32. The Commission lacks authority to require the use of certain tools, to compel the adoption of specific risk management practices, or to dictate the personnel decisions of companies in connection with cybersecurity.

[45] Unisys Order at paragraph 19.

[46] The U.S. Supreme Court is considering this issue in a pending case. *See Facebook v. Amalgamated Bank*, No. 23-980.

[47] *See* Modernization of Regulation S-K Items 101, 103, and 105, Release No. 34-89670 (Aug. 26, 2020) [85 FR 63726 (Oct. 8, 2020)] at section D, available at https://www.federalregister.gov/documents/2020/10/08/2020-19182/modernization-of-regulation-s-k-items-101-103-and-105 (https://www.federalregister.gov/documents/2020/10/08/2020-19182/modernization-of-regulation-s-k-items-101-103-and-105).

[48] Unisys Order at paragraph 18.

[49] *Id*.

[50] *Id*.

[51] *Id*.

Last Reviewed or Updated: Oct. 23, 2024