PUBLISHED OCTOBER 2024

SEC Cybersecurity Disclosure Requirements and Related Directors & Officers Liability Risks

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policy makers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

SEC Cybersecurity Disclosure Requirements and Related Directors & Officers Liability Risks

Published October 2024

Cybersecurity and the reporting of cybersecurity incidents by publicly traded corporations to investors is becoming an increasingly regulated arena. The United States Securities and Exchange Commission's (SEC) new cybersecurity incident reporting requirements for publicly traded companies in the United States is another move toward increased transparency surrounding material cybersecurity incidents.

This paper will:

1. Outline the details around the SEC's cybersecurity incident disclosure requirements;
2. Highlight some of the trends associated with the filings since the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule[1] became effective on December 18, 2023, and
3. Discuss the potential financial risks toward organizations surrounding inaccurate or misleading disclosure, including but not limited to securities class action lawsuits.

Outside of the Cyber Insurance line of business, potential financial losses such as SEC Fines and Securities Class Action Settlements impact the fiduciary and executive liability lines of business, most notably within Directors & Officers Liability Insurance.

Securities and Exchange Commission Disclosure Requirement

The SEC's new 8-K cybersecurity reporting requirement for material cyber incidents took effect on December 18, 2023. The disclosure rules require that publicly traded companies file an Item 1.05 Form 8-K within four business days of determining that a cybersecurity incident is material.[2] Previously, corporations would file Form 8-Ks to inform investors about cybersecurity incidents, but this new rule codified the four-business-day reporting timeline for material incidents.

1 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"; U.S. Securities and Exchange Commission; September 5, 2023.
2 "Cybersecurity Disclosure"; U.S. Securities and Exchange Commission; December 14, 2023.

For the actuarial community that monitors the frequency and potential financial magnitude of material cyber incidents, this new reporting requirement has the potential to bring about more timely information as well as greater transparency into cybersecurity risks.

In addition to the disclosure of material cybersecurity incidents, the SEC also required disclosure of an organization's cybersecurity risk management, strategy, and governance within its annual 10-K for U.S. corporations or 20-Fs for foreign private issuers.[3] This requirement went into effect for companies with fiscal years ending on or after December 15, 2023.

Clarification to the requirement

The Form 8-K cybersecurity reporting requirement led to many Item 1.05 Form 8-K disclosures by companies after December 18, 2023. However, many companies articulated that it was unclear whether an event would have a material financial or operational impact on the company. The Item 1.05 disclosure was specifically meant for the disclosure of cybersecurity incidents that were determined to be material. In fact, the title of Item 1.05 is "Material Cybersecurity Incidents." This nuance led to a clarification from the SEC on May 21, 2024, in which the SEC articulated that the cybersecurity incidents for which the materiality determination had not been made or for which the incident was immaterial be made under an Item 8.01 rather than the Item 1.05.[4] This delineation and distinction between a Form 8-K filing that is an Item 1.05 (material) versus Item 8.01 would better inform investors and allow for investors to distinguish between those incidents that are and are not material.

Cybersecurity Incident 8-Ks Filed After December 18, 2023

The following table shows the 22 entities that have filed 8-K forms with the SEC between December 18, 2023, and May 31, 2024. Some of these entities have filed subsequent 8-K updates, and the filings below are related to the initial 8-K filing. Of the 22 filings, five of the 22 were filed as 8.01 filings and 17 were filed as 1.05 filings. It's important to note that there were two filed after the SEC's updated guidance on May 21, 2024, and both of those filings were 8.01 filings.

3 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"; U.S. Securities and Exchange Commission; September 10, 2024.
4 "Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents"; U.S. Securities and Exchange Commission; May 21, 2024.

Review of the details contained in these filings (and amended Form 8-K filings) show that only three companies (loanDepot, VF Corporation, and Brandywine) made filings disclosing details around cyber insurance or any financial considerations. However, companies have disclosed some of the financial details within other earnings releases and financial statement filings such as 10-Q and 10-K filings. For those three filings with disclosed details around cyber insurance or financial considerations, loanDepot stated that the incident *would* have a material impact to its first-quarter 2024 results,[5] and it disclosed the costs of the incident net of expected insurance recoveries. The other two companies, VF Corporation[6] and Brandywine,[7] articulated that they had cyber insurance in place but did not state the amount of the insurance limits. Furthermore, First American Financial Corporation filed an amended Form 8-K stating that it expected the incident to have a material impact on its fourth-quarter 2023 results of operations. However, it did not state any financial impacts within that filing.[8]

Entity	Form 8-K Item Type	Initial Filing Date
Live Nation Entertainment, Inc.	Item 8.01	05/31/2024
Kulicke & Soffa Industries, Inc.	Item 8.01	05/28/2024
Key Tronic Corporation	Item 1.05	05/09/2024
Brandywine Realty Trust	Item 1.05	05/07/2024
DocGo Inc.	Item 8.01	05/07/2024
Dropbox, Inc.	Item 1.05	05/01/2024
Frontier Communications Parent, Inc.	Item 1.05	04/18/2024
OraSure Technologies Inc	Item 1.05	04/12/2024
B. Riley Financial, Inc.	Item 1.05	04/08/2024
Radiant Logistics, Inc.	Item 1.05	03/20/2024
Marinemax, Inc.	Item 1.05	03/12/2024
Federal Home Loan Bank Of New York	Item 1.05	03/01/2024
Cencora, Inc.	Item 1.05	02/27/2024
UnitedHealth Group	Item 1.05	02/22/2024
Prudential Financial, Inc	Item 1.05	02/13/2024
SouthState Corporation	Item 1.05	02/09/2024
Willis Lease Finance Corporation	Item 8.01	02/09/2024
Hewlett Packard Enterprise Company	Item 1.05	01/24/2024
Microsoft Corporation	Item 1.05	01/19/2024
loanDepot, Inc.	Item 8.01	01/08/2024
First American Financial Corporation	Item 1.05	12/22/2023
VF Corporation	Item 1.05	12/18/2023

5 loanDepot Form 8-K/A; U.S. Securities and Exchange Commission; January 4, 2024.
6 V.F. Corp. Form 8-K/A; U.S. Securities and Exchange Commission; December 15, 2023.
7 Brandywine Realty Trust Form 8-K/A; U.S. Securities and Exchange Commission; May 1, 2024.
8 First American Financial Corp. Form 8-K/A; U.S. Securities and Exchange Commission; December 20, 2023.

SEC Fines and Penalties

Before the 8-K material cybersecurity incident reporting rules went into effect on December 18, 2023, publicly traded corporations had a requirement via the SEC to provide appropriate disclosure to investors surrounding cybersecurity and privacy incidents. The SEC has fined companies in past instances in which the SEC found that companies did not disclose relevant information to investors in a timely manner, misled investors with their disclosures, or had internal control failures around the reporting of such incidents.

The table below outlines some of the fines and penalties levied by the SEC against organizations for their violations of these rules. The examples in the table below are limited to those related to cybersecurity and/or data privacy incidents.

Entity	Reason	Date	Fine / Penalty/ Settlement
Altaba (Yahoo!)	Failure to Disclose	04/24/2018	$35 million
Facebook	Misleading Disclosure	07/24/2019	$100 million
First American Financial Corporation	Disclosure controls and procedures violations	06/15/2021	$487,616
Pearson plc	Misleading Disclosure	08/16/2021	$1 million
Morgan Stanley Smith Barney	Failures to Safeguard Personal Information	09/20/2022	$35 million
Blackbaud	Misleading Disclosure	03/09/2023	$3 million
SolarWinds Corporation	Internal Control Failures/ Misleading Investors	10/30/2023	TBD
R.R. Donnelley	Disclosure and Internal Control Failures	06/18/2024	$2.1 million

Securities Class Actions

In addition to fines and penalties directly enforced by the SEC, publicly traded companies also face the risk of securities class action lawsuits from their shareholders. While many securities class actions related to cybersecurity and privacy incidents are dismissed, like the Marriott securities class action was,[9] the success by the plaintiffs and the settlement amount received in the examples below provide incentives for shareholders to pursue litigation against the companies.

As the insurance provider of a publicly traded company, a potential risk is a situation in which an insurance carrier may be participating on both the Cyber Insurance program and the Directors & Officers Liability Insurance program. In this situation, the given carrier could be impacted twice from the same underlying incident due to the correlated nature of the event driven securities litigation.

Notable Securities Class Action Settlements From Cybersecurity/Privacy Incidents

Entity	Loss Type	Approximate Settlement Date	Settlement
Yahoo!	Securities Class Action	03/02/2018	$80 million
Yahoo!	Derivative Lawsuit	01/04/2019	$29 million
Equifax	Securities Class Action	02/13/2020	$149 million
SolarWinds	Securities Class Action	11/28/2022	$26 million
Google	Securities Class Action	02/06/2024	$350 million
Okta	Securities Class Action	06/11/2024	$60 million

9 "Fourth Circuit Affirms Dismissal of Marriott Data Breach-Related Suit;" The D&O Diary; April 26, 2022.

Additional Actuarial Considerations

As previously articulated, the timely disclosure of material cybersecurity incidents by publicly traded companies may provide the actuarial community with additional data points for analyzing both the frequency and severity of such material incidents. While there was previously a requirement by companies to provide investors with pertinent information that may impact their investing decisions, the codification of the four-day timeline after determination of a material incident creates greater consistency for reporting across these publicly traded companies in the U.S.

Shifting from the cybersecurity and Cyber Insurance lens to Directors & Officers Liability Insurance reminds us that these cybersecurity incidents have the potential to impact more than one line of business for insurers—both as the insured if the company is publicly traded and as the insurer if participating on the Cyber Insurance and Directors & Officers Liability Insurance program for the impacted company. The potential severity of the fines, penalties, and class action settlements shown in the SEC Fines and Penalties and Securities Class Actions sections demonstrate the financial magnitude that these issues can bring to impacted companies. Due to this potential severity impacting both Cyber Insurance and Directors & Officers Liability Insurance, insurers would benefit from continuing to evaluate their aggregate risk exposure across these two lines of business—especially their aggregate exposure from the same corporation and similar industry sectors.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**