FORM 8-K

Analysis of recent cyber 8-Ks

How do public companies disclose cyber incidents

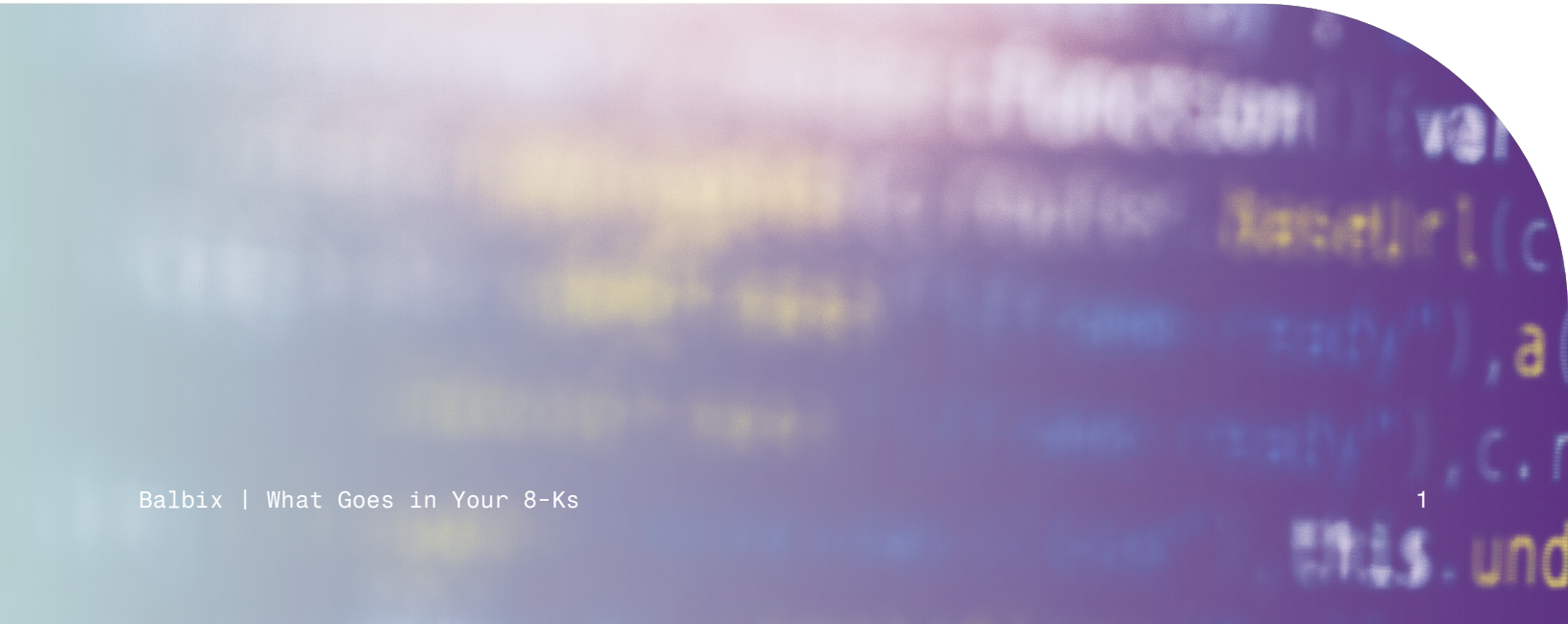
Balbix®

Summary

We analyzed 532 8-Ks filed by public companies between Jan 1, 2023, and Oct 12, 2023, to help CISOs, CFOs, and others understand what should and shouldn't go in their 8-Ks. While 8-Ks filed after July 26, 2023, provide the most meaningful information, the older 8-Ks provide historical context on what's changed.

Through this analysis, we gained insights into the language, timeline of disclosure, materiality threshold, and impact of these disclosures. While companies are not yet required by the SEC to disclose material cybersecurity incidents, many are doing so voluntarily, and we believe that these insights can help other companies structure their 8-K as they prepare to comply with the SEC's cybersecurity rule. While SEC cybersecurity disclosures aren't enforced yet, we hope this information can be useful to those looking to stay ahead of the curve.

We analyzed 532 8-Ks filed by public companies between Jan 1, 2023, and Oct 12, 2023.



Insights

Language of Disclosure(s)

After evaluating 8-Ks across several organizations, we have observed a trend toward standardization in the language used to disclose data breaches and disruptions. The term ‘cybersecurity incident’ is now commonly used to refer to potential incidents.

Previously, organizations used more specialized terms like ransomware, phishing, and denial-of-service attacks. However, it is worth noting that these specific terms are still being used in forward-looking statements. Standardizing language across the industry is a positive development as it helps streamline investor communication and understanding of cybersecurity. From a business perspective, investors are less concerned with the specific cause of the incident and more focused on the financial impact on revenue and expenses.

The Number and Timeline of Disclosure(s)

Before July 26, organizations were not obliged to adhere to specific timelines when disclosing cybersecurity incidents. The time frame for disclosure varied, with some companies reporting incidents just a few days after they occurred while others took several weeks. Most companies had no best practices without any regulations or processes for disclosing incidents, except for organizations subject to regulatory compliance, such as the Health Insurance Portability and Accountability Act (HIPAA).

The companies that disclosed cybersecurity incidents after July 26 have done so much faster. More specifically, between 0 and 7 days.

The companies that disclosed cybersecurity incidents after July 26 have done so much faster. More specifically, between 0 and 7 days, after the incident was deemed material. Many of these organizations go one step further, providing deeper insights into the incidents through subsequent 8-K disclosures, including the incidents' impact on key areas such as customer experience, supply chain, order processing, and top-line revenue.

While this demonstrates that some organizations are prepared to meet the SEC's 4-day disclosure requirements, others who have made no disclosures have a long way to go. Given the number of public companies and the frequency of cybersecurity incidents, we expected the number of 8-Ks filed in the last two-and-a-half months to be much higher.

A Word on Materiality

Over the years, the SEC has released several bulletins to clarify what constitutes "material" information. For instance, the SEC's cybersecurity rule outlines that an incident is considered "material" if the description contains information that a reasonable shareholder would likely find important when making an investment decision. Ultimately, it is the responsibility of individual organizations to determine what information is material to them. Through analyzing publicly available data in 8-K disclosures, we have attempted to quantify the concept of materiality. On average, incidents that negatively impacted annual revenue by 0.7% or more were disclosed. While the dataset of companies disclosing their revenue impact is small, it is a meaningful insight. While you may need to quantify materiality for your organization, consider this a data point in your assessments.

Impact of Incidents

Recent 8-K disclosures provide details on the potential impact of a cybersecurity incident on revenue and expenses. These incidents caused disruptions in the supply chain, order processing, bookings, and reservations. Further, many of these incidents caused margin

On average, incidents that negatively impacted annual revenue by 0.7% or more were disclosed.

compression due to one-time expenses related to investigations, remediation, notifications, fines, and penalties. In a few cases, companies were able to offset their losses with cyber insurance coverage.

While some companies provide a dollar figure impact on gross profit, others simply mention its impact on earnings-per-share. Regardless of the method chosen, investors need to understand the impact of the cybersecurity incident through 8-K or subsequent 10-Q/10-K disclosures.

Parting Thoughts

It is concerning to note that there are approximately 6,000 publicly traded companies, and cyberattacks remain a common occurrence, with numerous systems being compromised daily. It begs the question of the small number of 8-K disclosures made daily.

Assuming that each company experiences at least one significant cybersecurity incident per year (though the number is likely higher), we should expect to see between 20-30 cybersecurity-related 8-K filings every business day.

However, we see fewer 8-Ks filed. While it is possible that some companies are adopting a wait-and-watch approach and are not required to disclose incidents yet, most companies are likely not adequately prepared to detect and disclose "material incidents."

Data Analysis

To compile this report, we read & analyzed 532 8-Ks, 8-K 99.1, 99.2, 10-Q, and 10-K filed by hundreds of U.S.-based public companies between Jan 1, 2023, and Oct 12, 2023. A subset of those organizations in our sample size are included below.

We focused mainly on disclosures made after July 26's SEC ruling to provide insights into how other public companies are filing their 8-Ks. The list includes public disclosures by Freeport McMoran, Maximus, MGM, Caesar, Clorox, Johnson Control, Conagra Brands, Tempur Sealy, PROG Holdings, Simpson Manufacturing, and Garret Motion.

In contrast, we also looked back to the beginning of this year to understand if there has been a change in the speed or language of disclosures. Those that filed 8-K before July 26 include Estée Lauder, Hayes, Heico, Enzo Biochem, Tecogen, NCR, PGT, Lumen, QuickLogic, MKS, Americold Reality, and Trico Bancshares.

Additionally, we reviewed 8-K and 10-Q disclosures from firms such as Blackbaud, Radiant Logistics, T-mobile, PCB Bancorp, Interface Inc, and Jackson Financials, who disclosed their incidents at different times in 2023 for incidents that occurred in 2022 or earlier, which we acknowledged, but ignored for this analysis.

Finally, we analyzed several other companies that didn't have an actual incident but mentioned cybersecurity incidents or attacks in their disclosures. We found these mentions were part of standard risk disclosures, and there were no actual incidents. These were part of our dataset but did not influence our findings.