MARCH 2023

CYBER-SECURITY BREACH DISCLOSURES

HOW EXISTING REPORTING COMPARES TO THE ENHANCED DISCLOSURE RULES EXPECTED FROM THE SEC - **TIMELY REPORTING MAY NEED EXTRA ATTENTION**

MYLOGIQ

TABLE OF CONTENTS

"A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."

SEC Chair Gary Gensler
March 9, 2022

ENHANCED DISCLOSURE RULES ON THE HORIZON

With the expected April 2023 announcement from the U.S. Securities and Exchange Commission (SEC) of finalized rulemaking to enhance disclosure of cybersecurity risk management, we took a look at current reporting practices to see where things stand and to help provide guidance on where companies need to go once the new rule becomes effective.

5 AREAS OF DISCLOSURE FOCUS

The proposed rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* has five areas of disclosure focus:

- Incident Disclosure
- Timeliness of Incident Disclosure
- Board Oversight
- Board Expertise
- Management Policies & Procedures.

This report looks at disclosure practices for the first four of these areas.

METHODOLOGY

Using our CompanyIQ SEC disclosure research platform, we reviewed the 8-K current event filings of all Russell 3000 index companies from January 2022 to February 2023 to identify cybersecurity incident filings. We also used the CompanyIQ ESG and corporate governance databases to identify disclosed information on board cybersecurity oversight and expertise. We identified 28 companies that reported a cybersecurity breach during the 13-month study period.[1]

The findings in this report are based on the publicly disclosed reporting of these 28 companies.

KEY FINDINGS

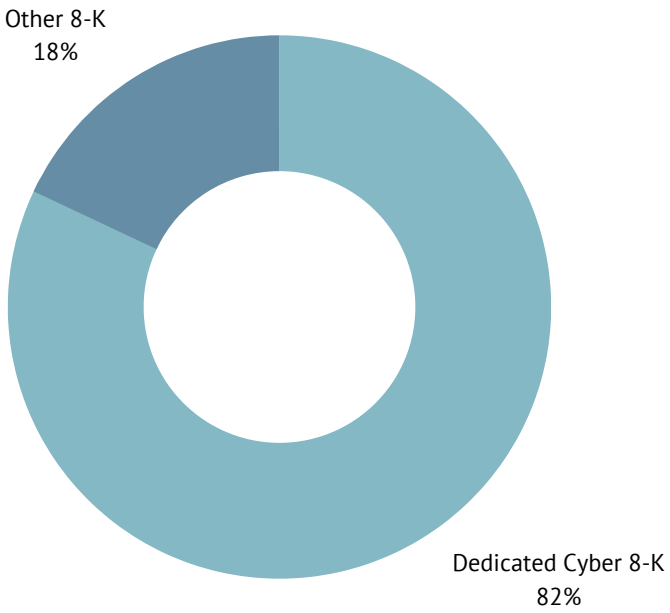
- 82% Use a Dedicated 8-K for Incident Disclosure
- Nearly 50% Did Not Disclose the Nature of the Incident
- **Less Than 50% Disclosed in 4 Days**
- 71% Assign Cybersecurity Oversight to Their Audit Committee
- 7% of Directors Have Cybersecurity Expertise
- 32% of Companies Have Cybersecurity Expertise on Their Boards
- 89% Are Large Accelerated Filers
- 30% Are Technology Companies

[1]Three of the study companies reported breaches that related to a subsidiary, a contractor, and a third-party vendor.

INCIDENT DISCLOSURE- PART 1

Dedicated 8-Ks for Cybersecurity Incidents Are the Norm

Almost all of the 28 study companies, 23 or 82%, provided a dedicated 8-K to publicly report their cybersecurity incident.

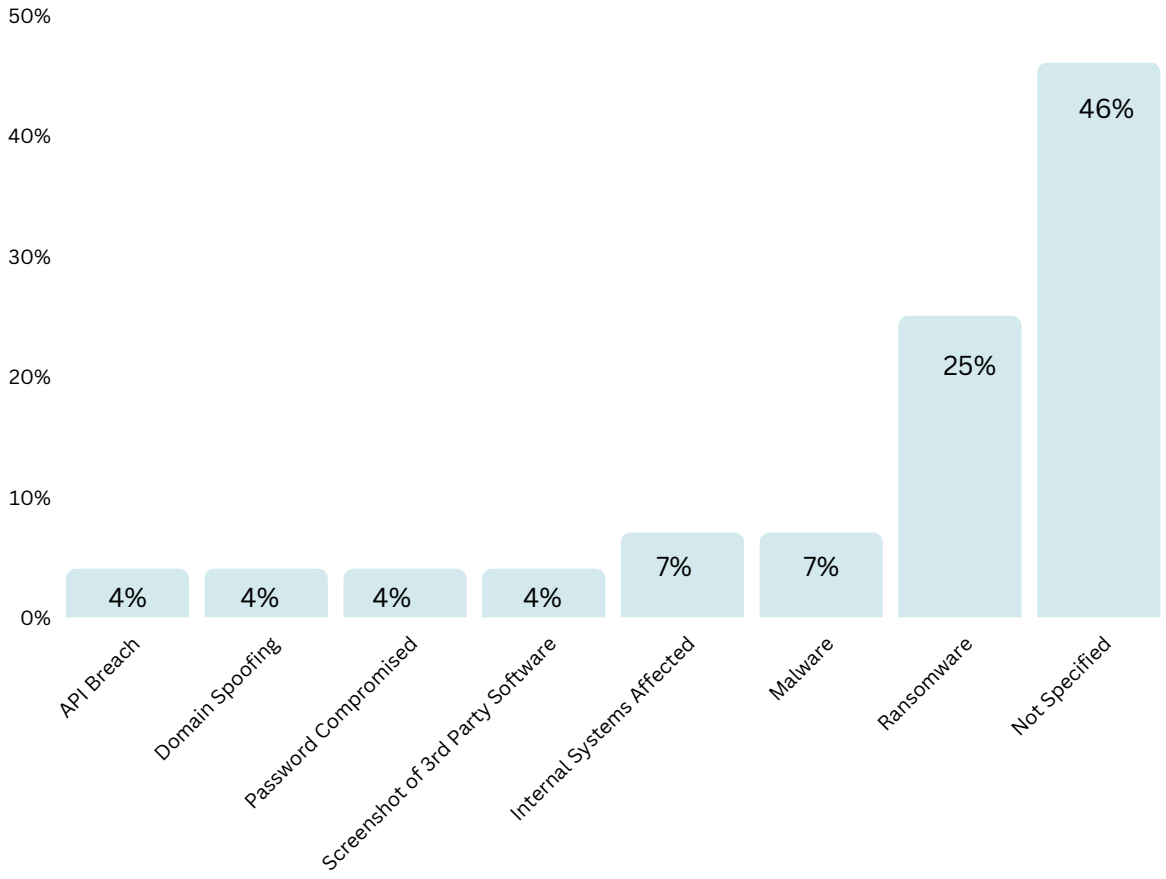


The five study companies without a dedicated cyber incident 8-K relied on earnings release or financial results 8-Ks. One of the five reported the incident in a 8-K exhibit related to financial results.

INCIDENT DISCLOSURE - PART 2

Type of Incident

Nearly half of the 28 study companies, 13 or 46%, did not specify in their 8-K what type of cybersecurity incident they experienced.



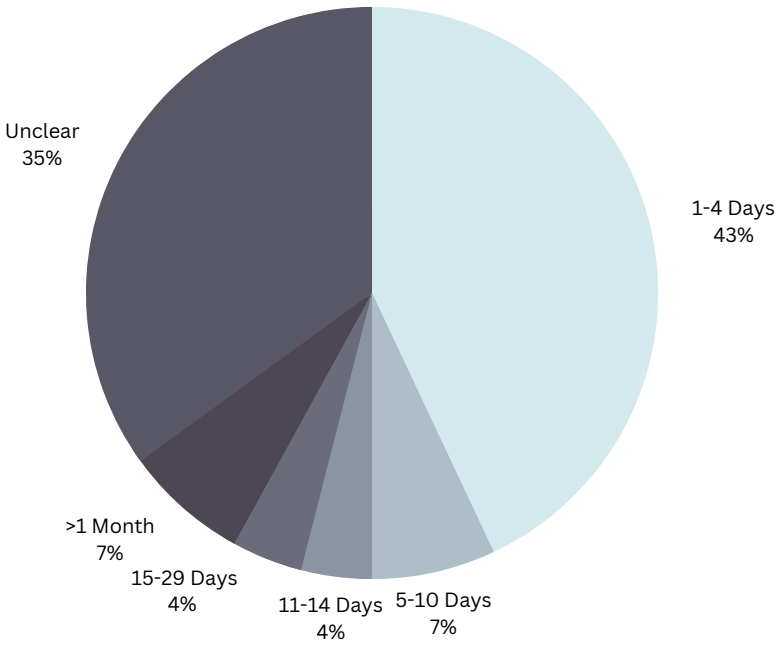
The next largest group, at 25%, reported ransomware as the cause of their cyber incident, followed by malware and internal systems affected both at 7% each.

TIMELINESS OF REPORTING

Less Than Half Met 4-Day Disclosure Standard

Less than half of the study companies met the SEC's proposed requirement of reporting cyber incidents within four business days.

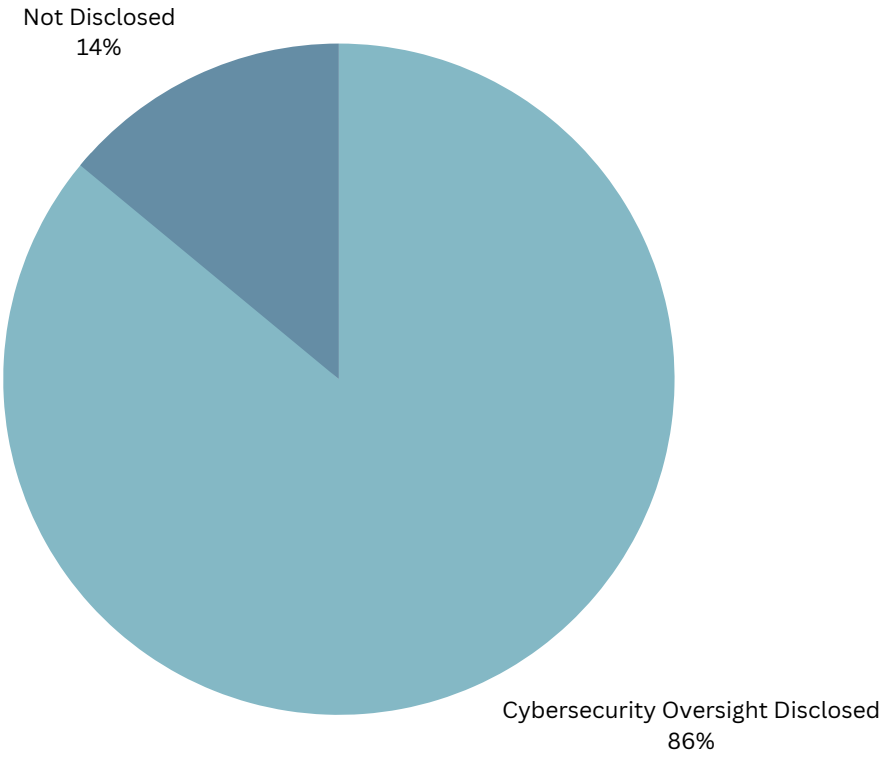
More than a third were unclear in their reporting about when the incident was discovered, thus making it difficult to determine the timeliness of their disclosures. And a few waited more than a month to report their incidents.



BOARD OVERSIGHT

Almost All Disclose Who is Responsible

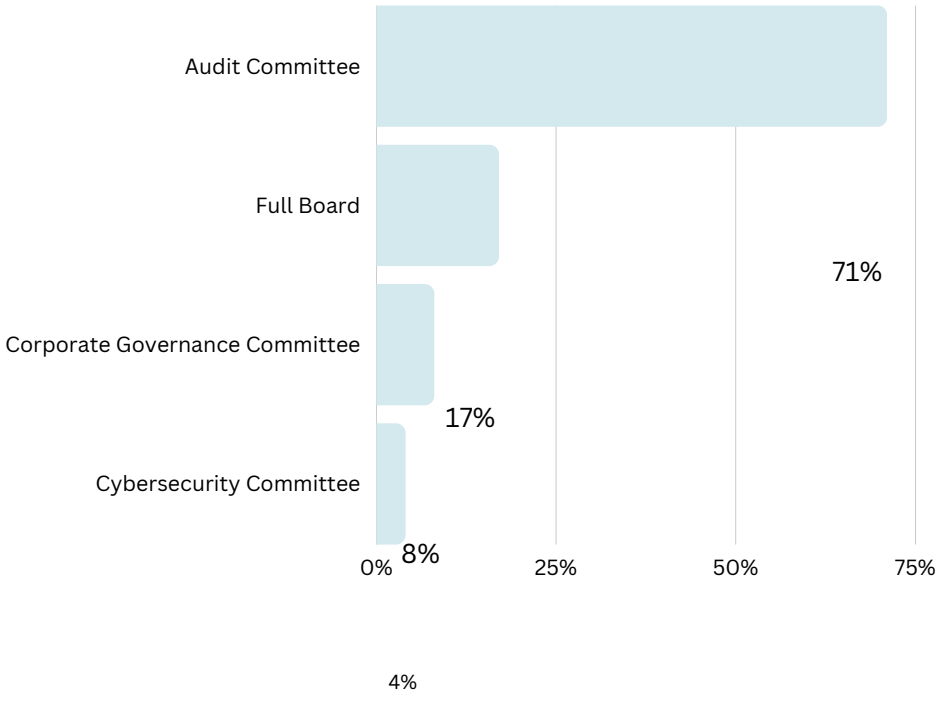
24 of the 28 study companies, or 86%, disclosed who has responsibility at the board level for overseeing cybersecurity.



BOARD OVERSIGHT (CONT.)

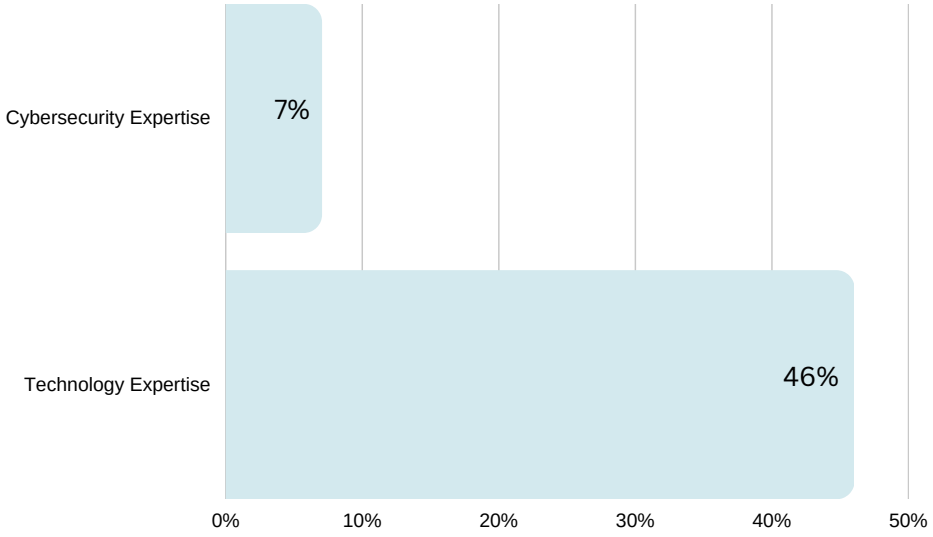
Audit Committee Still Dominates

17 of the 24 disclosing companies, or 71%, have assigned responsibility at the board level for overseeing cybersecurity to their Audit Committees.

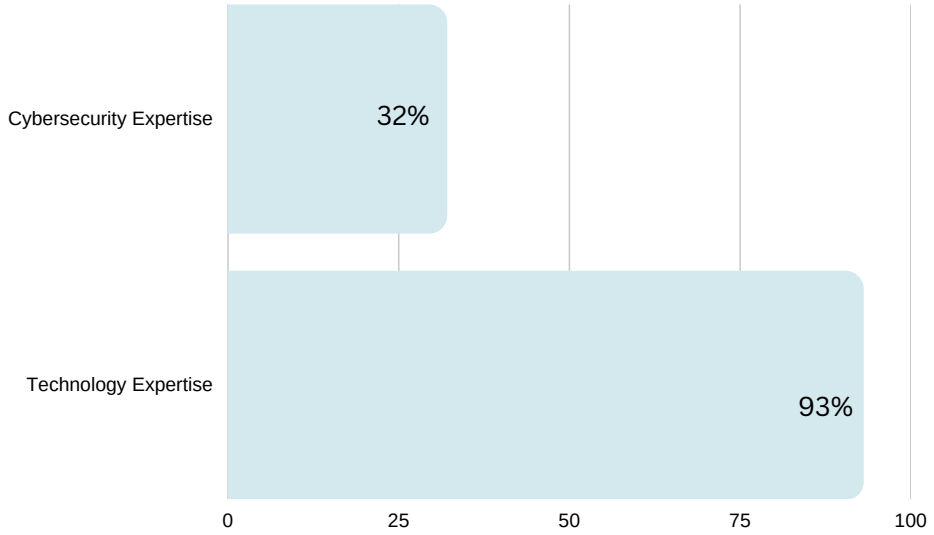


BOARD CYBERSECURITY EXPERTISE

Director Expertise



Company Expertise*

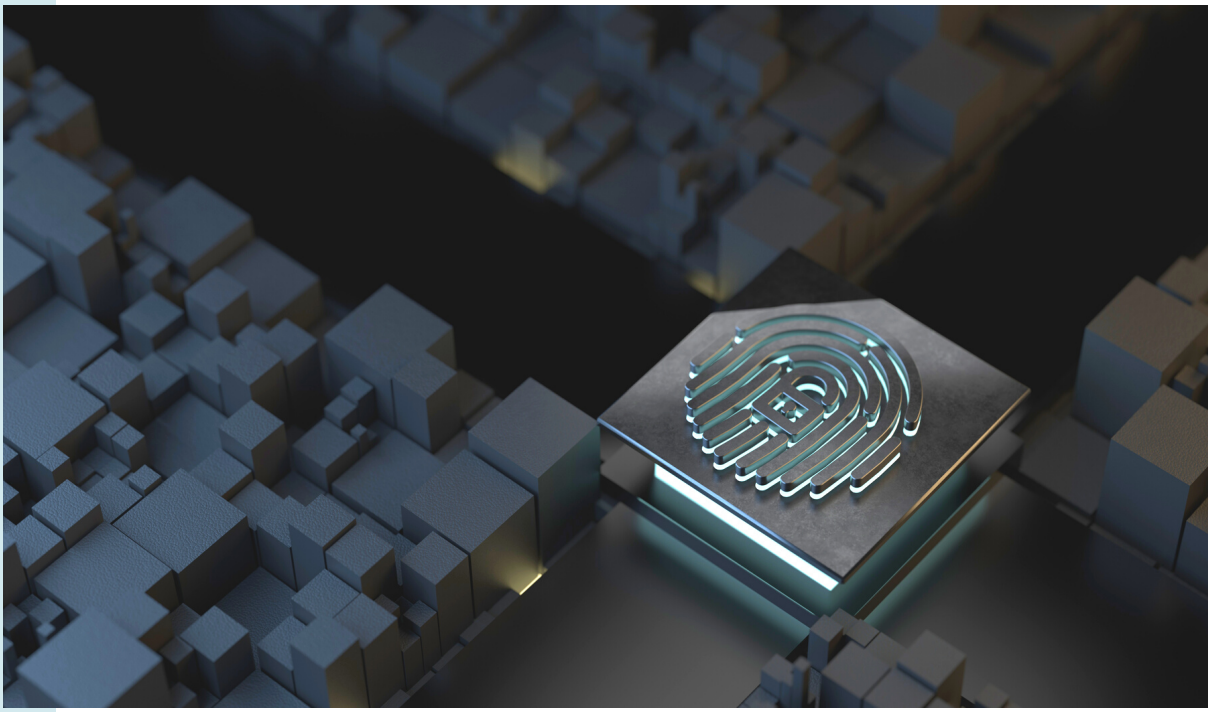


*At least one board member has this expertise.

DISCLOSING CYBERSECURITY EXPERTISE (CONT.)

As the first chart on p. 9 indicates, very few directors of the 28 study companies, 7%, have cybersecurity expertise. Considerably more, 46%, have general technology expertise.

The second chart on p.9 shows that 32% of the study companies have at least one director with cybersecurity skills. And 93% of the companies have at least one director with general technology skills.

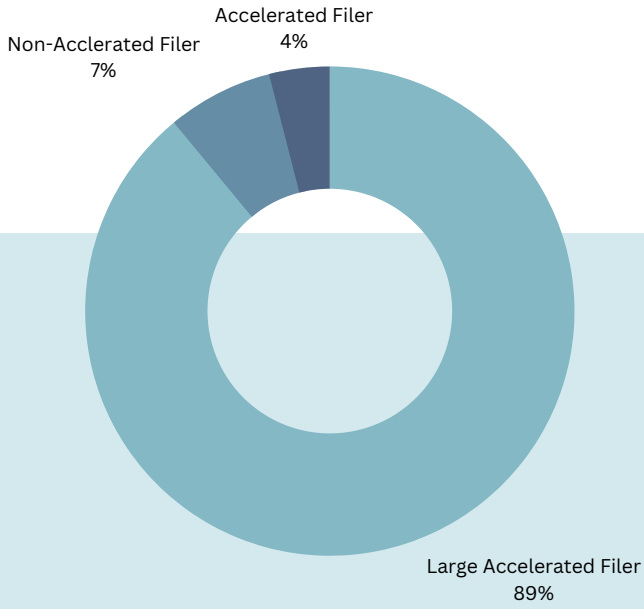


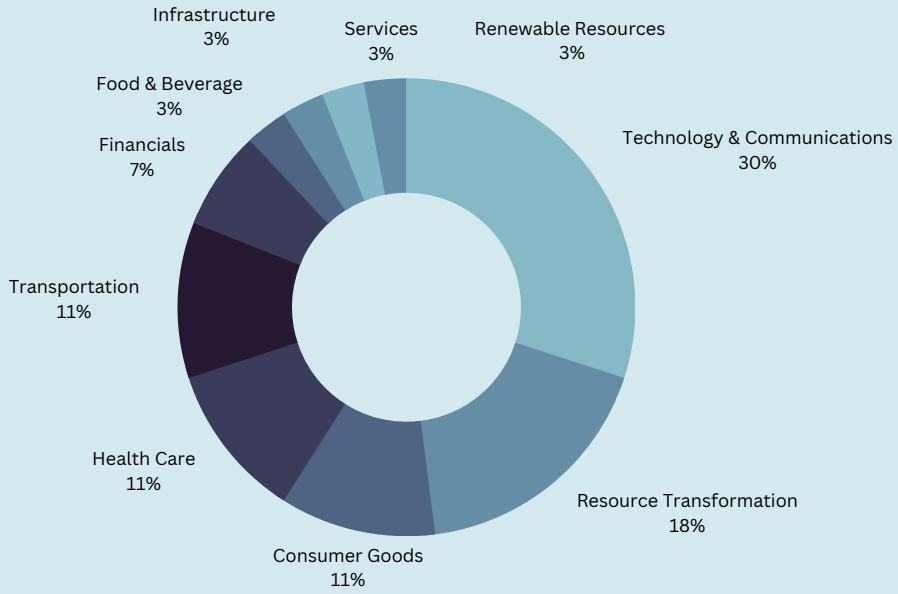
COMPANY PROFILES

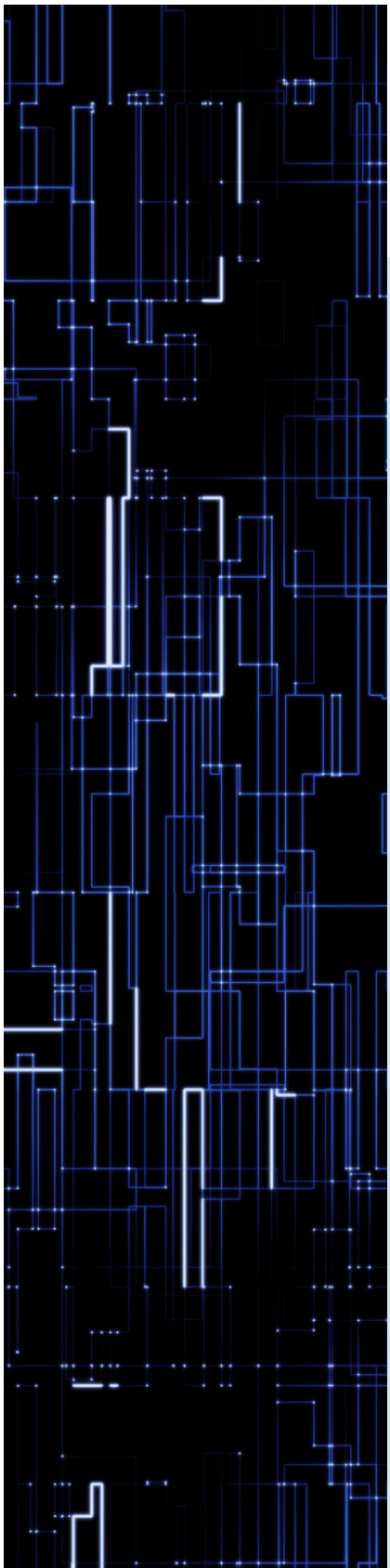
LARGE ACCELERATED FILERS IN THE TECHNOLOGY SECTOR MOST PREVALENT

The charts below provide an analysis of two profile elements for the 28 study companies.

- 89% are large accelerated filers.
- 30% are in the technology sector.







BENCHMARKING GUIDANCE FOR CYBER DISCLOSURES:

BEST PRACTICES

Based on our observations of R3000 cybersecurity disclosure data over the past 13 months, below are some benchmarking points that may suggest best practices:

1. File a separate 8-K dedicated to the incident.
2. File within 4 business days as the SEC has proposed.
3. Clearly disclose who is responsible at the board level for cybersecurity oversight.
4. Review whether the correct committee is overseeing cybersecurity at the board level.
5. Review whether you need to add a board member with cybersecurity expertise.

About MyLogIQ

MyLogIQ (www.mylogiq.com) provides 360°public company intelligence through our CompanyIQ® Answer Desk research platform. We offer an unrivaled AI-powered solution for benchmarking public companies with real-time access to research and analytics sourced from SEC filings and company websites on one platform. Our data covers:

- Climate Disclosures
- ESG
- Cybersecurity
- SEC Disclosures and Comment Letters
- Risk Factors, Accounting Standards, and MD&A
- Audit Fees & SOX
- Company ESG/CSR Reports, Committee Charters, & Governance Policies
- Proxy Proposals & Shareholder Engagement
- Corporate Governance
- Board Composition, Profiles, and Diversity
- Board & Executive Compensation.

Contact us to request a demo.