JULY 2024

EQUILAR

2024 Cybersecurity Disclosure Trends

An Equilar Publication

Featuring Commentary From

DFIN

Table of Contents

1100 Marshall Street, Redwood City, CA 94063
121 W Wacker Drive, Suite #1805, Chicago, IL 60601
1120 Avenue of the Americas, Suite #4045, New York, NY 10036

Phone: (650) 241-6600 | **Fax:** (650) 701-0993 | **E-mail:** info@equilar.com
www.equilar.com

Editor-in-Chief
Amit Batish

Lead Author
Joyce Chen

Data and Analysis
Sinem Atalay
MaryClare Colombo
Jeremy Ho
Erin Le

Design and Layout
Aileen Pan
Danny Shin

Executive Summary

As the world becomes increasingly connected through various networks and systems, protecting stored data has become a major concern. Cybersecurity, the practice of protecting systems, networks and data from digital attacks, is essential. Cyberattacks are often motivated by financial gain, aiming to steal money or data and disrupt businesses. Effective cybersecurity safeguards personal, financial and business information from unauthorized access and theft. It mitigates the risk of financial loss and protects businesses from disruptions caused by cyberattacks, allowing operations to continue smoothly. As a result, cybersecurity builds trust with customers and clients since a breach can heavily damage a company's reputation. Overall, it protects critical infrastructure and government systems from cyber espionage, sabotage and warfare, ensuring national security.

The latest Securities and Exchange Commission (SEC) regulations require United States-listed public companies to report cybersecurity incidents within four business days of discovery. This mandate is effective for the fiscal year ending on or after December 18, 2023. The regulation assumes that all organizations are susceptible to potential threats and breaches, highlighting the significance of this disclosure.

The new regulation primarily targets public companies. However, many public companies rely on private third-party software and services, which are even more vulnerable to cyberattacks. This interconnectedness means that the cybersecurity posture of third-party vendors is critical to the overall security of public companies. As a result, it is crucial for them to be aware and compliant with the new SEC regulations. However, this comes with challenges as third-party companies are often smaller and have less access to valuable cybersecurity resources.

The concept of the cyber poverty line (CPL), coined by Wendy Nather, former head of advisory CISOs at Cisco, divides organizations into two groups: those that have the resources to implement security measures and those that cannot. The CPL is a key indicator of smaller vulnerable companies, which is crucial as these companies often collaborate with larger corporations. Once a hacker gains access to a smaller third-party company, it becomes easier to infiltrate the larger corporation it works with. For example, in the 2013 Target breach, hackers infiltrated the system through a small HVAC company working with Target, ultimately breaking into the cash register system and stealing millions of customers' credit card information.

Other large corporations, such as Rite Aid and AT&T, have also faced major cyber-attacks affecting millions of customers. Rite Aid experienced a breach where an unknown third party impersonated an employee, acquiring customer data including names, addresses, dates of birth and IDs between June 2017 and July 2018. Additionally, AT&T discovered hackers had stolen call and text

logs of over 100 million customers, including phone numbers and call records. This breach also affected customers of Mobile Virtual Network Operators (MVNOs) using AT&T's network. These incidents compelled both large corporations to closely examine and enhance their cybersecurity measures in hopes that such catastrophe would not occur again.

Nevertheless, the threat of cyberattacks constantly looms, and companies must ensure they are taking the appropriate measures to prevent these attacks. Establishing a presence of leaders with cybersecurity expertise at the executive and board levels, along with transparent corporate cyber policies, are essential steps in the process. This Equilar publication, featuring commentary and insights from DFIN, identifies key trends in cybersecurity disclosures and how companies are addressing this critical issue.

A Glance at the Numbers

Over the last five years, the likelihood of companies disclosing a cyber incident was very low. During the study period, not a single Equilar 100 company disclosed an incident in 2019, 2020 and 2022. In 2023, just 5% of companies disclosed an incident. Of course, with the passing of the SEC's new cyber disclosure rules, this trend will be worth keeping an eye on over the next year or so, as the prevalence of disclosures will almost certainly spike. With regards to the new Item 1C section of the 10-K—where companies must provide details on their processes for assessing, identifying and managing material risks from cybersecurity threats—67% of Equilar 100 companies disclosed their policies in 2024 filings.

Meanwhile, the presence of cybersecurity committees is on the rise. In 2019 and 2020, only 1% of Equilar 100 companies had an established committee dedicated to cybersecurity. However, by 2023, this figure rose to 4%—the highest mark of the study period. Furthermore, the percentage of Equilar 100 companies that disclosed board-level cybersecurity risk oversight grew to 33% in 2023, a 307.4% increase from 8.1% in 2019.

The percentage of companies disclosing data privacy and cybersecurity policies remained constant at 6% in both 2022 and 2023, a stark contrast from 0% in 2019. Notably, 92.3% of Equilar 100 companies in the consumer defensive industry included cybersecurity disclosures in their reports for 2023—the highest among all industries in the study.

To effectively safeguard themselves from malicious cyberattacks, it is critical that companies have clear, actionable policies in place. Raising awareness about cyberattacks and remaining vigilant is key. Companies must ensure that they stay ahead of threats, and meeting the requirements set forth by the SEC and having the appropriate skills on their team will be deemed invaluable in the long term.

Industry-Leading Governance Insights

The Equilar Institute is a collection of thought leadership on topics related to executive intelligence, corporate governance and executive compensation. Stay up to date with our award-winning publications, webinars and blogs.

www.equilar.com/institute

Methodology

Cybersecurity Disclosure Trends, an Equilar publication, analyzes the proxy statements and Form 10-Ks of Equilar 100 companies from 2019 to 2023. The Equilar 100 tracks the 100 largest, by reported revenue, U.S.-headquartered companies trading on one of the major U.S. stock exchanges (Nasdaq, NYSE or NYSE American). Year one (2023) was defined as companies with a fiscal year ending from January 1, 2023 to December 31, 2023, and previous years were defined similarly. The publication examines key disclosure practices around cybersecurity policies and incidents, as well as the presence of cybersecurity experts on corporate boards. DFIN offers independent commentary on the state of cybersecurity governance and how companies should plan to address new SEC rules.

Key Findings

5%

Of companies disclosed a cyber incident in 2023, the highest mark of the study period.

44

Companies disclosed cybersecurity expertise for board members in both a skills section and in their bios in 2023, up from 12 in 2019.

33%

Of companies featured detailed disclosures on their boards' cybersecurity risk oversight in 2023, up from 8.1% in 2019.

92.3%

Of companies in the consumer defensive industry included cybersecurity disclosures—the highest among all industries.

Beyond the Numbers | DFIN

A Q&A With Ron Schneider, Director of Corporate Governance Services at DFIN

To provide additional insights on the trends uncovered in *Cybersecurity Disclosure Trends*, Equilar sat down with Ron Schneider, Director of Corporate Governance Services at DFIN. Schneider shared thoughts on the new cybersecurity disclosure rules announced by the SEC, as well as factors companies should consider when disclosing information pertaining to their cybersecurity policies. Below is a snapshot of the conversation. The full conversation with Schneider can be found at the end of this publication.

Equilar: What are the key expectations in regards to the new SEC cybersecurity disclosure rules. From an organizational level, how can the new rules impact future cyber risks and mitigate potential threats?

Ron Schneider: First, let's review the new rules: On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted rules requiring companies to:

- Disclose "material" cybersecurity incidents they experience within four days of determining its materiality. Also, describe the material aspects of the incident's nature, scope and timing—as well as its material impact or reasonably likely material impact on the company.
- Annually describe their cybersecurity risk management, strategy and governance (i.e. their processes to assess, identify and manage material cybersecurity risks). This specifically includes describing the board of directors' oversight of cybersecurity threats and risks.
- Importantly, as with traditional financial reporting, these new disclosures must be tagged within Inline eXtensible Business Reporting Language (iXBRL). Per the SEC, the iXBRL requirement begins one year after initial compliance and will make this information "more consistent, comparable and decision-useful."

These new rules became effective for Accelerated and Large Accelerated filers on December 15, 2023, and for Smaller filers on June 15, 2024. All registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

Those are the new reporting requirements. Potential benefits to companies in defending against future cyber-attacks and mitigating their impact may include:

- Taking a fresh look at their vulnerabilities and protections and upgrading and intensifying data protection, employee training and other efforts in these areas.
- Ensuring their management and board have the requisite levels of expertise. Where these are lacking, acquiring that expertise including intensifying training efforts.
- Reviewing peer company and other leading company disclosures to identify best practices they can apply to themselves.
- Developing and streamlining procedures for management to report relevant information to the board, to make timely decisions about potential materiality, and how they will report this information to regulators, investors, and affected individuals, customers and suppliers. The board (or designated committee) must be actively involved in this process.

SEC rule announcement: SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

DFIN Fact Sheet: Smaller Reporting Companies Must Comply with the SEC's Cybersecurity Rules | Donnelley Financial Solutions (DFIN) (dfinsolutions.com)

Equilar: How should companies balance compliance and transparency with the need to protect confidential information when disclosing cybersecurity incidents? What steps can be taken by companies to ensure appropriate compliance?

Schneider: This is more than a compliance exercise. Remember that trust and confidence in your company, its executive leadership and board can take years or even careers to develop, but can be damaged or dissolved with one misstep in this and other critical areas—whether strategic, operational or reporting.

The good news is that, in our experience, management teams and boards are taking this very seriously. Also, there is a constantly growing body of "best practice" peer and other company disclosures that companies can use to benchmark a) their procedures and controls, as well as b) their disclosures in these areas. Clearly, companies are finding ways to discuss and describe their vulnerabilities, preparedness and controls at a high level without giving away sensitive company, employee, customer or other information. And when it comes to preparedness, bear in mind that you only get credit for what you disclose!

- **Proactively**, companies should identify and pull together the appropriate cross-functional teams at the management and board levels, review their risks, preparedness and expertise, benchmark themselves against peers and other leading companies, and describe their cybersecurity preparedness, including management and board expertise in these areas. As an example, we are seeing a rapid increase in companies breaking out "cybersecurity" from overall "risk management" in proxy disclosures, including appropriate mentions in board bios, committee descriptions and responsibilities, oversight procedures, and skills matrices. Examples of these and other relevant disclosures can be found here: Guide to Effective Proxies - 11th Edition I DFIN I Donnelley Financial Solutions (dfinsolutions.com).
- **Reactively to an incident**, companies should make the appropriate disclosures in a timely fashion, being as transparent as they can at all stages of the threat occurrence, its identification, mitigation and material impact(s).
- Learn from the experiences of others. We suggest companies review the pre- and post-disclosures of companies that have experienced material cyberattacks with an eye toward upgrading their pre-disclosures. Also look at the disclosures of your key suppliers and customers—they will be looking at yours!

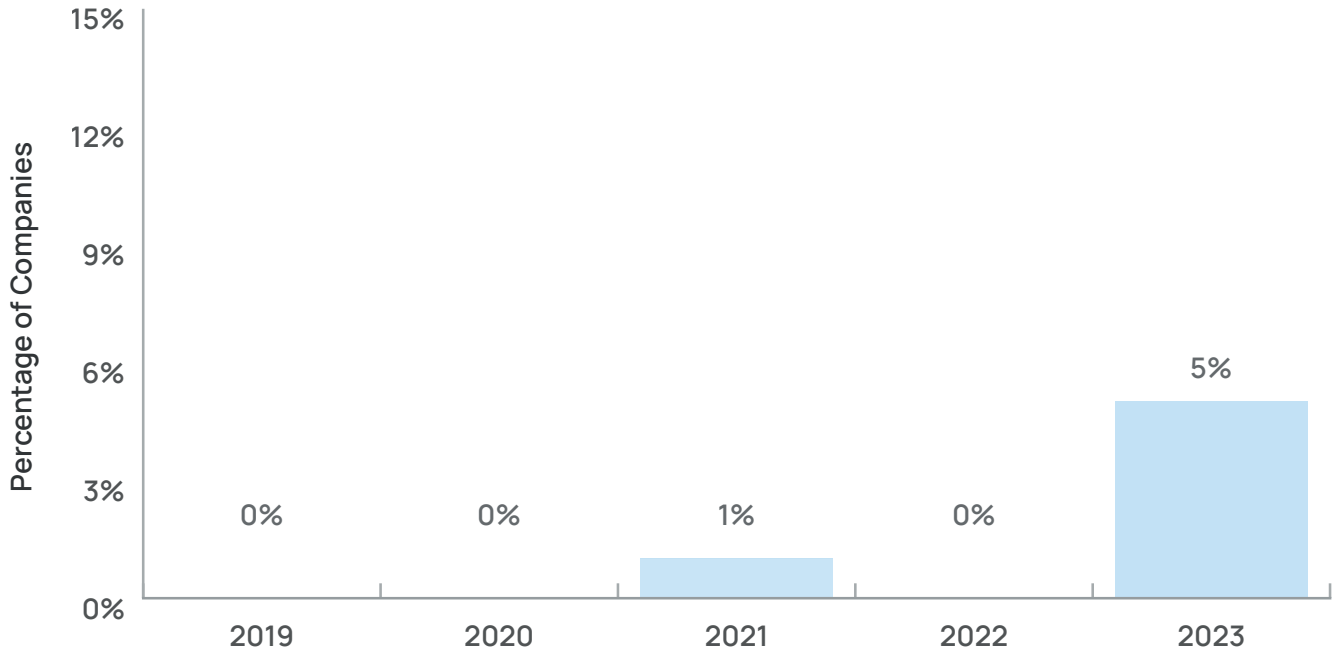
Read More From DFIN

Addressing Cybersecurity Across Corporate America

on page 15 of this report.

Fig. 01

Reporting a Cybersecurity Incident (Equilar 100)

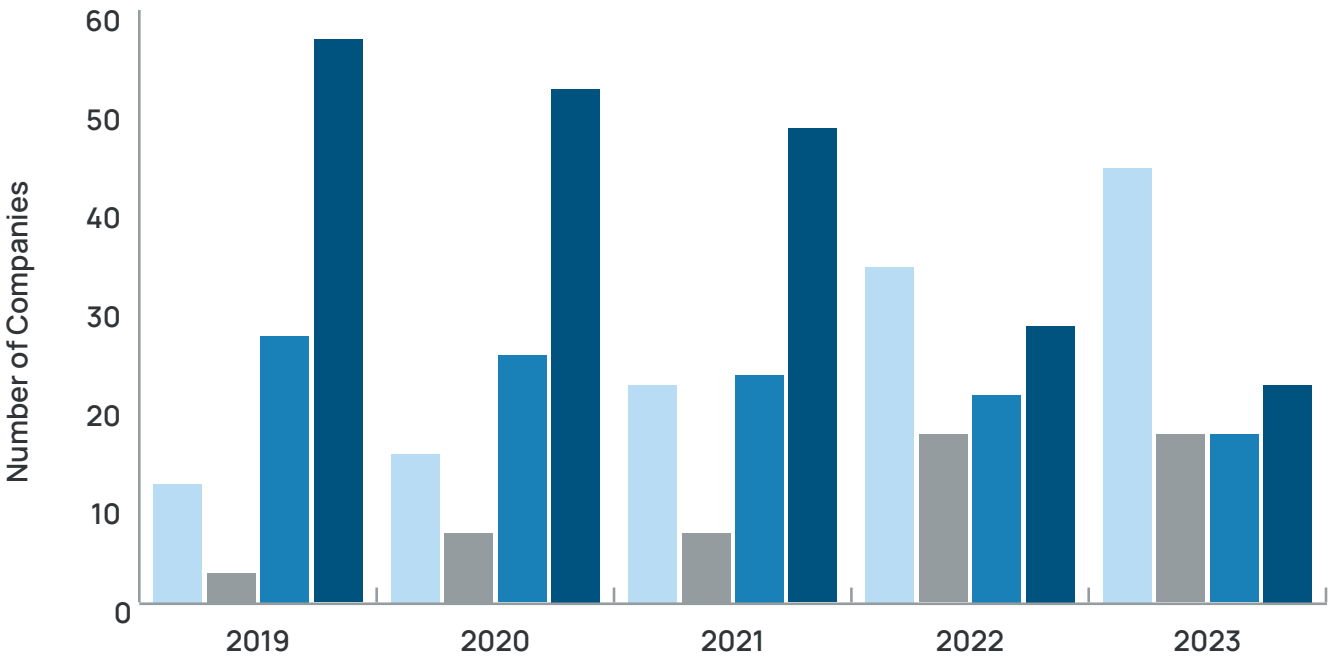


1. In 2019, 2020 and 2022, no Equilar 100 company reported a cybersecurity incident (Fig. 1)

2. In 2023, 5% of companies reported an incident—the highest in the study period (Fig. 1)

Fig. 02

Disclosures of Cybersecurity as Board Director Skill (Equilar 100)



	2019	2020	2021	2022	2023
Skills & Bio	12	15	22	34	44
Skills Only	3	7	7	17	17
Bio Only	27	25	23	21	17
None	57	52	48	28	22

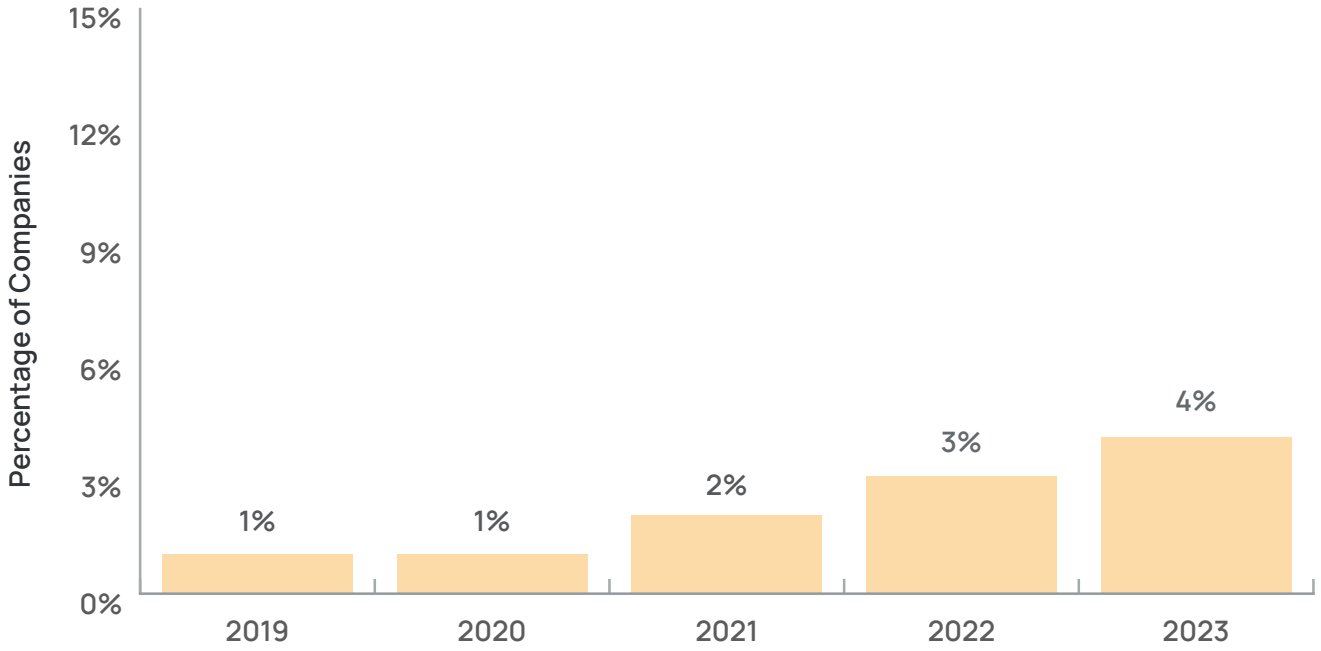
1. In 2019, the disclosure of board director skills and bios was uncommon, with 57 companies not disclosing and 42 disclosing (Fig. 2)

2. From 2019 to 2023, the number of Equilar 100 companies disclosing cybersecurity expertise for board members in both a skills section and in their bios increased by 267%, from 12 to 44 (Fig. 2)

3. The number of companies that did not disclose any board members with cybersecurity expertise dropped by 61.4%, from 57 to 22 (Fig. 2)

Fig. 03

Companies With a Cybersecurity Committee (Equilar 100)

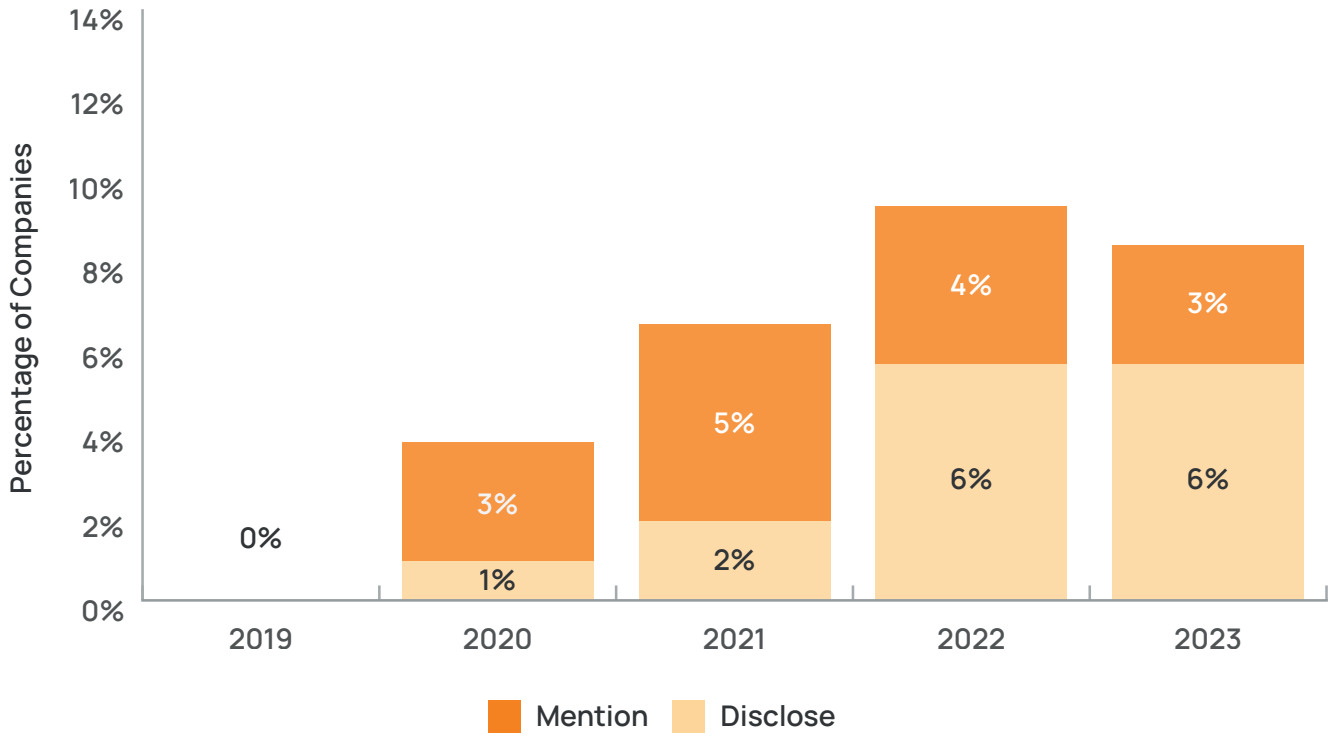


1. In 2019 and 2020, only 1% of Equilar 100 companies had a cybersecurity committee; by 2021, this percentage increased to 2% (Fig. 3)

2. In 2023, the percentage of companies with a cybersecurity committee reached its highest level during the study period (4%) (Fig. 3)

Fig. 04

Disclosing Data Privacy and Cybersecurity Policies (Equilar 100)



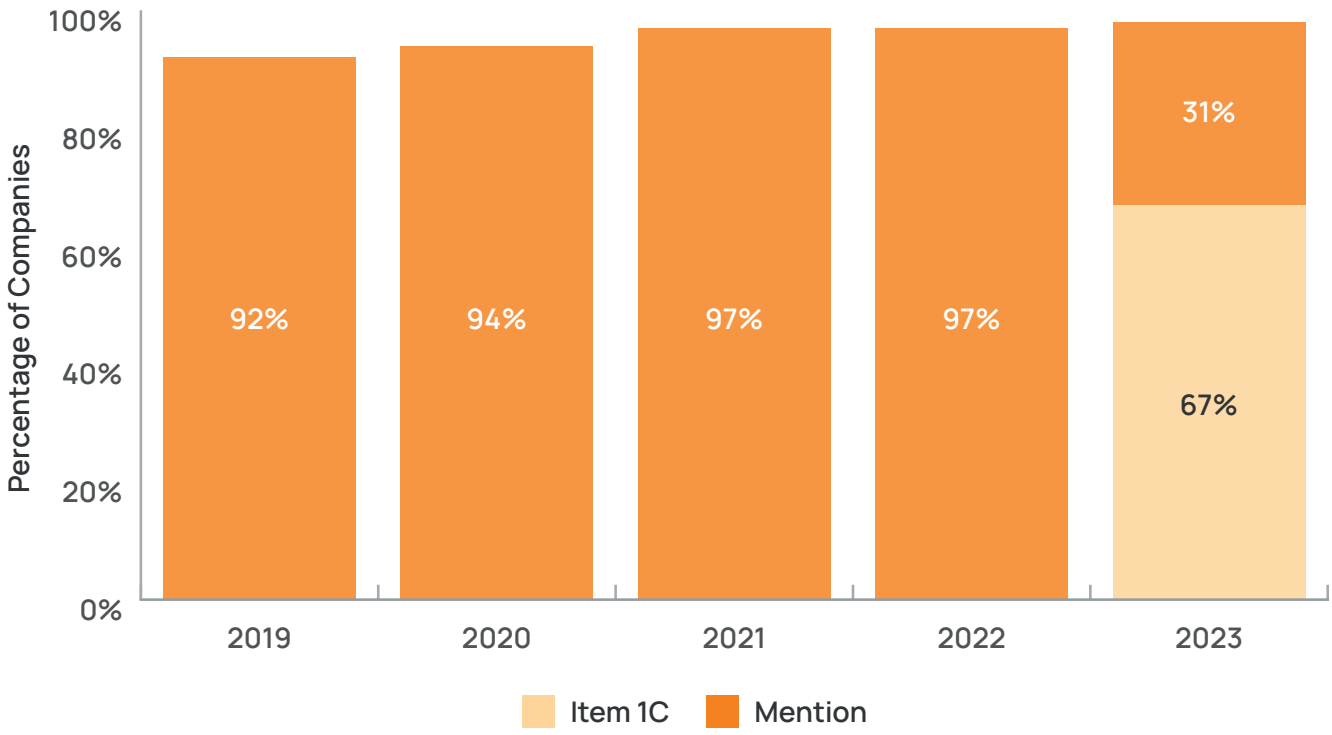
1. The highest percentage of companies featuring some degree of information on data privacy and cybersecurity policies was in 2022 at 10% (Fig. 4)

2. The percentage of companies disclosing data privacy and cybersecurity policies remained constant at 6% in both 2022 and 2023 (Fig. 4)

3. None of the Equilar 100 companies disclosed or mentioned data privacy and cybersecurity policies in 2019 (Fig. 4)

Fig. 05

10-K Cybersecurity Disclosures (Item 1C) (Equilar 100)



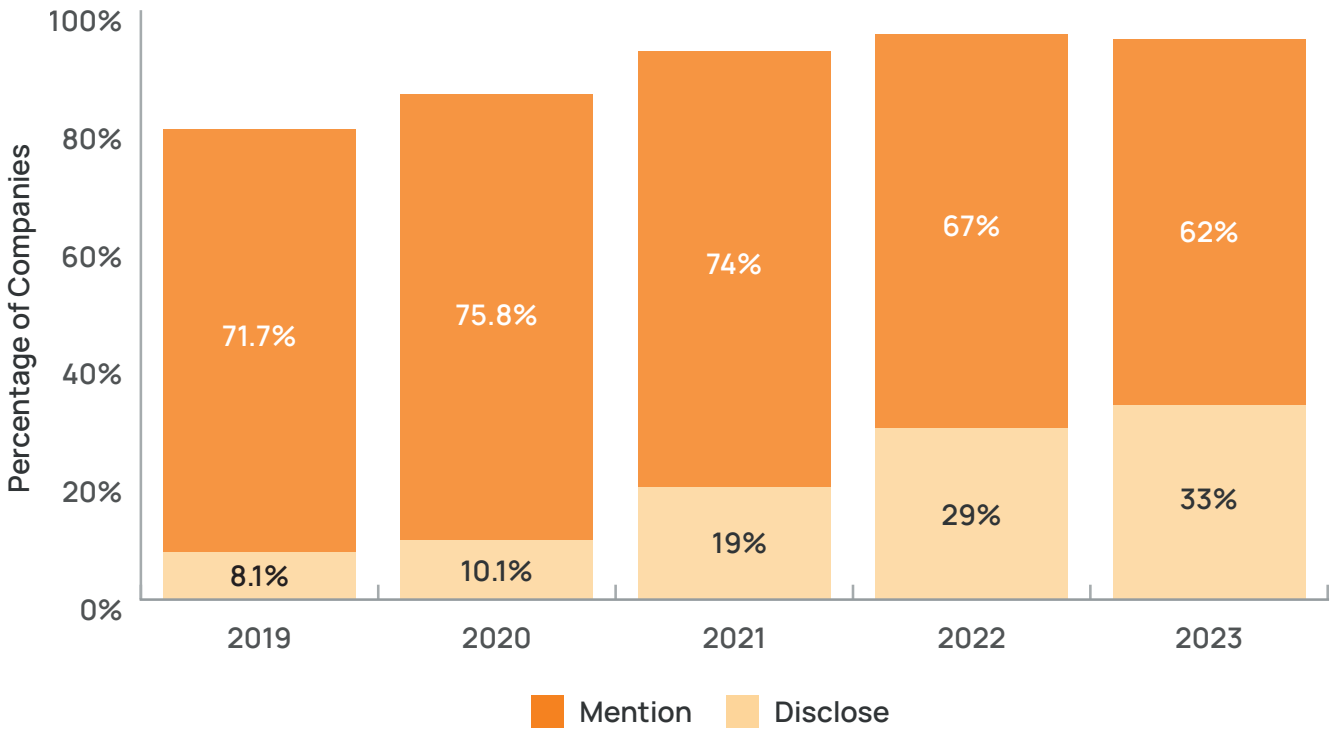
1. In 2019 and 2020, just under 95% of Equilar 100 companies mentioned cybersecurity to some degree in their 10-K forms (Fig. 5)

2. In both 2021 and 2022, 97% of Equilar 100 companies included mentions of cybersecurity on their 10-K forms (Fig. 5)

3. Following the implementation of the SEC's cybersecurity rules, 67% of companies disclosed cybersecurity in the Item 1C portion of their 10-K forms (Fig. 5)

Fig. 06

Disclosing Board Cybersecurity Risk Oversight (Equilar 100)

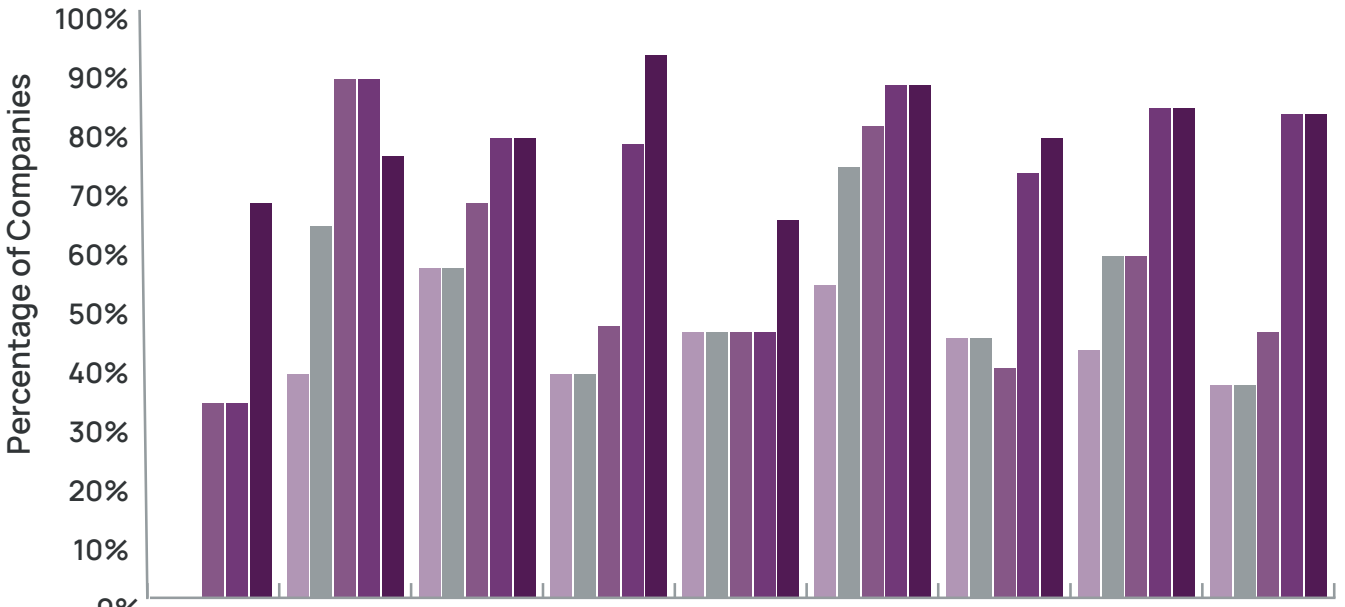


1. In 2023, 95% of Equilar 100 companies included information on their boards' cybersecurity risk oversight, up from 79.8% in 2019 (Fig. 6)

2. In 2022, 96% of companies included their boards' cybersecurity risk oversight, the highest mark during the study (Fig. 6)

Fig. 07

Cybersecurity Disclosures by Industry (Equilar 100)



	Basic Materials	Comm. Services	Consumer Cyclical	Consumer Defensive	Energy	Financial Services	Healthcare	Industrials	Technology
2019	0.0%	37.5%	55.6%	38.5%	45.5%	53.3%	44.4%	41.7%	36.4%
2020	0.0%	62.5%	55.6%	38.5%	45.5%	73.3%	44.4%	58.3%	36.4%
2021	33.3%	87.5%	66.7%	46.2%	45.5%	80.0%	38.9%	58.3%	45.5%
2022	33.3%	87.5%	77.8%	76.9%	45.5%	86.7%	72.2%	83.3%	81.8%
2023	66.7%	75.0%	77.8%	92.3%	63.6%	86.7%	77.8%	83.3%	81.8%

1. In 2023, 92.3% of Equilar 100 companies in the consumer defensive industry included cybersecurity disclosures—the highest among all industries (Fig. 7)

2. The energy industry remained steady at 45.5% of companies from 2019 to 2022, only to increase to 63.6% in 2023 (Fig. 7)

3. The basic materials industry saw the largest increase in cybersecurity disclosures in the study period, rising from 0% of companies in 2019 to 66.7% in 2023 (Fig. 7)

Disclosure Example | AMERICAN EXPRESS | Filed March 15, 2024

The following examples are exceptional instances of cybersecurity disclosures from the proxy statements of American Express and General Motors. The two companies provide detailed information regarding their policies, as well as key measures their teams are taking to prevent cyber attacks.

Compensation and Benefits Committee

- Works with the Chief Colleague Experience Officer and the Chief Risk Officer to ensure our overall compensation programs, as well as those covering our business units and risk-taking employees, appropriately balance risk with business incentives and that business performance is achieved without taking imprudent or excessive risk
  - Our Chief Risk Officer is actively involved in setting risk goals, including for our business units
  - Our Chief Risk Officer also reviews the current and forward-looking risk profiles of each business unit and provides input into performance evaluations
  - Our Chief Risk Officer meets with the committee and attests as to whether performance goals and results have been achieved without taking imprudent risks
- Uses a risk-balanced incentive compensation framework to decide on our bonus pools and the compensation of senior executives
- Approves the charter of, and receives reports from, Management's Risk Performance & Incentive Review Committee that reviews whether certain risk outcomes warrant downward adjustment to incentive compensation

Cybersecurity Oversight and Risk Management

We maintain an information security and cybersecurity program and a cybersecurity governance framework that are designed to protect our information systems against cybersecurity risks. Information security and cybersecurity risk is an operational risk that is measured and managed as part of our operational risk framework. Operational risk is incorporated into our comprehensive Enterprise Risk Management (ERM) program, which we use to identify, aggregate, monitor, report and manage risks. Our Board receives an update on cybersecurity at least once a year and our Risk Committee receives reports on cybersecurity at least twice a year, including in at least one joint meeting with the Audit and Compliance Committee, and our Board and these committees all receive ad hoc updates as needed. In addition, the Risk Committee annually approves the Company's Technology Risk and Information Security (TRIS) program described below.

Our TRIS program, which is our enterprise information security and cybersecurity program incorporated in our ERM program and led by our Chief Information Security Officer (CISO), is designed to (i) ensure the security, confidentiality, integrity and availability of our information and information systems; (ii) protect against any anticipated threats or hazards to the security, confidentiality, integrity or availability of such information and information systems; and (iii) protect against unauthorized access to or use of such information or information systems that could result in substantial harm or inconvenience to us, our colleagues or our customers. The TRIS program is built upon a foundation of advanced security technology, employs a highly trained team of experts and is designed to operate in alignment with global regulatory requirements. The program deploys multiple layers of controls, including embedding security into our technology investments, designed to identify, protect, detect, respond to and recover from information security and cybersecurity incidents. Those controls are measured and monitored by a combination of subject matter experts and a security operations center with integrated cyber detection, response and recovery capabilities. Cybersecurity risks related to third parties are managed as part of our Third Party Management Policy, which sets forth the procurement, risk management and contracting framework for managing third-party relationships commensurate with their risk and complexity.

TRIS Program Highlights

- We have a Cyber Crisis Response Plan in place that provides a documented framework for handling high-severity security incidents and facilitates coordination across multiple parts of the Company
- We invest in threat intelligence and are active participants in industry and government forums
- We collaborate with our peers in the areas of threat intelligence, vulnerability management and incident response and drills
- We routinely perform simulations and drills at both a technical and management level
- We incorporate external expertise and reviews in our program
- Colleagues receive annual cybersecurity awareness training

We continuously assess the risks and changes in the cyber environment and adjust our program and investments as appropriate. For more information on our cybersecurity risk management, strategy and governance, see "Item 1C. Cybersecurity" of our 2023 Annual Report on Form 10-K.

Cybersecurity Risk Oversight

Material risks from cybersecurity threats are managed across GM, GM Financial, Cruise, and third-party suppliers and vendors, and monitoring such risks and threats is integrated into the Company's overall risk management program. In addition, the Board has assigned its Risk and Cybersecurity Committee with the specific responsibility for overseeing cybersecurity threats. The Company's cybersecurity organization is led by the Chief Cybersecurity Officer ("CCO"), who is responsible for assessing and managing material risks from cybersecurity threats and reports to GM's Executive Vice President, Legal, Policy, Cybersecurity, and Corporate Secretary, as well as to the Risk and Cybersecurity Committee. GM also has a Cybersecurity Management Board that brings together representatives from senior management across the Company's Software and Services, Product Development, Information Technology, Manufacturing, Finance, Communications, Human Resources, Legal, and Public Policy organizations to provide guidance and monitor overall company cybersecurity risk. The Company's cybersecurity maturity scorecard, cybersecurity threats, and certain incident information are reviewed by the CCO, the Risk and Cybersecurity Committee, and the Cybersecurity Management Board during standing meetings, as well as in impromptu sessions, when appropriate. During the reviews, various topics are discussed, which may include:

- implementation and maturity of the Company's cybersecurity program, risk management framework, including cybersecurity risk policies, procedures, and governance;
- cybersecurity and privacy risk, including potential impact to the Company's employees, customers, supply chain, joint ventures, and other stakeholders;
- intelligence briefings on notable cyber events; and
- cybersecurity budget and resource allocation, including industry benchmarking and economic modeling of various potential cybersecurity events.

The CCO and the Cybersecurity Management Board monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents through their management of, and participation in, the cybersecurity risk management processes described above, including through the operation of the Company's incident response plans, which include escalation to the CCO and the Cybersecurity Management Board, as appropriate.

A Deep Dive | DFIN

Addressing Cybersecurity Across Corporate America

A Q&A with Ron Schneider, Director of Corporate Governance Services at DFIN

Equilar: As seen in the study results, the prevalence of companies that have a board director with cybersecurity skills has steadily risen in the last five years. How critical is it for companies to have that skill and expertise on the board, particularly in this era?

Ron Schneider: It's a must have! The range of issues and risks that boards must be prepared to effectively oversee is expanding rapidly, as is investor scrutiny of board expertise in these areas. Recent additions to board oversight responsibilities include sustainability and human capital efforts, cybersecurity, AI (and who knows what's next).

Most companies report intensifying their board education efforts through briefings and accreditations from outside experts, as well as regular presentations from management, including the chief information security officer(CISO) reporting on their security assessments, security measures and identified incidents. Here, we note that Canadian issuers have long surpassed their U.S. counterparts in the depth of their disclosures about ongoing board education efforts.

Some companies have also chosen to go the route of securing one or more "specialist" directors with specific expertise in these areas. For a good review of this trend, its pros and cons, see this recent academic study: Specialist Directors.

Equilar: On the flipside, are you surprised to see that just 4% of companies have a cybersecurity committee? Do you anticipate this number to rise in light of the SEC rule?

Schneider: No, I am not surprised at this current level of dedicated committees, but I do think it will gradually increase in particularly vulnerable or scrutinized sectors. Whether it involves the full board, the audit or other traditional committee, or a newly commissioned (or re-named) committee, companies increasingly are being clear and specific about where cybersecurity oversight (as well as that of other emerging risks) lies.

And as stated earlier, disclosure of board competencies in this area is intensifying, including in director bios (in part turbo-charged by the new Universal Proxy rules), skills matrices and elsewhere.

Equilar: Are there specific industries or sectors that you believe will be impacted more than others by the new SEC rules? If so, how should these industries tailor their disclosure practices?

Schneider: As a major institutional investor stated at a recent conference I attended, "when it comes to cybersecurity, EVERY company is a technology company!" This simply reflects the fact that all companies have technology platforms housing their employee, customer and other data, and these are vulnerable to financially motivated ransomware and other attacks.

As reported in a recent BlackBerry Global Threat report:

Most Attacked Industries in Cyberspace

Overall, the top five industries targeted by cyberattacks are:

1. Finance (50% of attacks)
2. Healthcare (20%)
3. Government & Public Sector (18%)
4. Food (4%)
5. Utilities (4%)

"Big-game hunting" is a term you will hear often, as larger companies may have the most at-risk data, as well as the greatest financial means to pay ransom (including various levels of cyber-threat insurance protection).

- Financial firms have the potential for substantial financial gains, given their significant customer data and funds.
- Healthcare companies play a significant societal role and have great amounts of patient healthcare data. Utilities similarly play a significant role in society and

public safety.

- Government and agencies may be tempting targets from both financial and geopolitical standpoints.

But remember—no company is immune!

Equilar: What are some key lessons companies can learn from previous cybersecurity incidents that can enhance their disclosure around their policies in the future?

Schneider: Whether the incident(s) occurred at their own company, an industry peer, supplier, customer or other large visible company, it's important to benchmark your procedures, controls, training, expertise and other measures against those of others as evidenced by their public disclosures.

Look at both the pre- and post-disclosures of impacted companies for insights into additional measures—and disclosures—you can apply pre-incident at your own company.

You cannot be too prepared. If you feel comfortable with your current level of preparation and security, share the high-level aspects of that publicly (i.e. "take credit"), but don't be cocky as nobody is immune!

Review both the procedures and disclosure of board oversight and expertise in these areas. It's surprising but as documented in the earlier cited *Specialist Director* paper, the same director may have different types of expertise cited by different companies on whose boards they serve. This may make sense where different skills are deemed more important at different companies, but this cross-comparison deserves a fresh look.

Equilar: How do you believe these new disclosure requirements will affect investor relations, if at all, and the manner in which companies communicate with their shareholders about cybersecurity risks and incidents?

Schneider: Investors are often the "canary in the coal mine" regarding emerging risks and areas of focus. I remember 30 + years ago when a new question investors were asking companies was "what is your internet strategy?"

IROs (as well as the CEO, CFO and board members involved with investor engagement) are at the front lines of this dialogue. Now, in addition to traditional questions about company strategy and performance ("where are you now, where are you headed and how will you get there?"), depending in part on their industry and stage of growth, investors may ask about sustainability efforts, commitments and outlook, employee development efforts, and increasingly, cyber-preparedness as well as AI risks and opportunities.

So, it doesn't really change the nature of the IRO's role and responsibilities, but rather it's yet another significant area over which the IRO and other investor-facing individuals must be prepared to articulate the company's best (and true) story—as well as to report back to senior management and the board on these evolving areas of investor interest.

About the Contributor

Donnelley Financial Solutions (DFIN) is a leading global risk and compliance solutions company. We provide domain expertise, enterprise software and data analytics for every stage of our clients' business and investment lifecycles. Markets fluctuate, regulations evolve, technology advances, and through it all, DFIN delivers confidence with the right solutions in moments that matter.

Learn about DFIN's end-to-end risk and compliance solutions online at DFINsolutions.com or you can also follow us on X @DFINSolutions or on LinkedIn.

Additional proxy disclosure examples, similar to those found in this publication, can be found in DFIN's Guide to Effective Proxies, 11th edition.

Ron Schneider

Director of Corporate Governance Services
Donnelley Financial Solutions (DFIN)

Ron joined DFIN as Director of Corporate Governance Services in April 2013. He is responsible for providing thought leadership on emerging corporate governance, proxy and disclosure issues.

Over the past four decades, Ron has advised senior management, the C-suite and boards of public companies of all sizes, industries and stages of growth facing investor activism, as well as challenging and sensitive proxy solicitations involving corporate governance, compensation and control issues.

His primary recent focus has been helping companies conduct engagement programs with their top institutional investors with the objective of identifying and addressing investor concerns through best practices in proxy disclosure.

At DFIN, Ron works closely with clients and our firm's sales and service teams to identify and implement appropriate changes to proxy statement design, content and navigation that fit each client's unique corporate culture and proxy-related objectives.

During his career he has managed more than 1,600 proxy solicitations, 200 tender or exchange offers and 30 proxy contests, with his proxy fight clients succeeding in over 70% of such situations.

Ron earned a B.A. in Economics from Princeton University.

HAVE YOU MET ERIC?

Equilar Research Intelligence Copilot

Your AI Disclosure Analyst

"What are the executive ownership guidelines stock holding requirements?"

"Do companies provide excise tax gross-ups to their executives upon CIC?"

"What events trigger recoupment under executive clawbacks?"

EQUILAR INSIGHT

Learn more at **www.equilar.com/ERIC**