CompanyIQ™ Cybersecurity & Board Oversight Intelligence Report

October 26, 2018

reports@mylogiq.com

©2018, MyLogIQ LLC

All Rights Reserved.

Data in this document is provided for informational purposes only and is subject to change without notice. It is not intended to add, replace, or remove any obligation of MyLoGIQ under a license or any other written agreement in place between MyLoGIQ and the recipient. By accepting this document, the recipient agrees not to copy, modify, adapt, translate, or otherwise alter the document without the express written consent of MyLogIQ, unless such right pre-exists under a license or other written agreement between MyLogIQ and the recipient.

Introduction

New interpretive guidance from the Securities and Exchange Commission (SEC) in February 2018 makes it clear that staff there will be paying increased attention to cybersecurity risks and how well publicly traded companies are disclosing them.[1]

Concern among investors, customers, and regulators about data protection and infrastructure safety continues to grow. A robust cybersecurity program where responsibility starts at the top with a company's board is a key indicator of how US companies are managing the risk that a cyberattack poses.

The SEC commissioners themselves have also signaled their view on cybersecurity when SEC Commissioner Robert Jackson Jr. said earlier this year that, "Cybersecurity is the most important corporate governance issue we face. There is no greater threat to businesses than cyber-attacks."[2]

Others have put it more starkly.[3]

With 121 million new malware programs discovered in 2017 alone, the threat of a US company experiencing a cyberattack is real.[4]

> **"The single biggest existential threat that's out there, I think, is cyber."**
>
> Ret. Adm. Michael Mullen, former Chairman of the Joint Chiefs of Staff.

[1] SEC Statement and Guidance on Public Company Cybersecurity Disclosures February 26, 2018.
[2] Remarks of SEC Commissioner Robert Jackson Jr at the 2018 National Conference of the Society for Corporate Governance, June 21, 2018.
[3] The Conference Board, "23 Truths About Cybersecurity – Insights from the Cybersecurity Conference: Crucial Collaborations," January 2018.
[4] As reported in The Wall Street Journal, September 18, 2018, "How AI Can Help Stop Cyberattacks," Adam Janofsky, citing a study by the AV-Test Institute www.av-test.org/en/statistics/malware.

Our report looks at how US publicly traded companies are managing their cyber risk and how they are reporting on what they are doing.

To do this our CompanyIQ™ platform analyzed:

- the trailing 15 months of proxy filings,
- more than 3,300 companies across eight sectors,
- the Dow 30,
- the S&P 100, S&P 400, S&P 500, and S&P 600, and
- the Russell 1000, Russell 2000, and Russell 3000.[5]

We identified some startling statistics relating to cybersecurity disclosure along with several eye-opening trends in disclosure and governance best practices.

Some of our major findings with our AI-augmented platform are that:

- nearly a quarter of S&P 100,
- more than a third of S&P 500, and
- more than half of Russell 3000 companies either:
  - have little to no board oversight for cybersecurity, or
  - have not done a good job of communicating their oversight.

No Disclosure of Board Oversight on Cybersecurity:

- **1/4 of S&P 100**
- **1/3 of S&P 500**
- **3/5 of Russell 3000**

"Either way it begs the question if countries allegedly hack elections, what risks do these companies foresee? Hope is not a strategy," notes Ganesh Rajappan Founder & CEO, MyLogIQ LLC.

[5] Some indices are subsets of others or overlap. As such, company totals may not match.

Executive Summary

- ***62% of the Russell 3000 & 33% of S&P 500 Did Not Disclose if They Have Board Oversight of Cybersecurity:*** 1,766 of the companies on the Russell 3000 and 166 of the S&P 500 companies did not mention cybersecurity oversight in their proxy filings.[6] (Chart 1, p.7)

- ***Some Notable Companies Have Not Disclosed:*** The list is long but here are a few. Exxon Mobil from the Dow 30, BNY Mellon, Abbott Labs, Costco, PayPal, and hundreds of other large companies appear to have made no effort in disclosing any oversight.

- ***Audit Committees Reign Over Cybersecurity in the S&P 500:*** Nearly two-thirds of the 334 S&P 500 companies that place cybersecurity oversight with their board do it through their audit committees. However, three-quarters of the audit committee members of these companies do not indicate any technology skill. (Chart 6, p. 15)

- ***Pharmaceutical and Life Sciences Companies in the S&P 500 Appear Most at Risk:*** Pharmaceutical and life sciences companies lead the sectors, in percentage terms, that do not disclose if they have board responsibility for cybersecurity. (Chart 14, p.25)

- ***Only 11 Have a Dedicated Cybersecurity Committee:*** Our analysis shows that only 11 of the more than 3,300 companies we reviewed disclosed a dedicated cybersecurity committee at the board level. (Table 1, p. 10)

[6] There is no mention regarding cybersecurity oversight or related terms in the company's proxy.

Methodology

In order to determine a company's stated oversight of cybersecurity risk, we analyzed more than 3,300 companies in eight indices of US publicly traded companies as of October 26, 2018.

The source documents were the latest released company proxies, corporate governance guidelines, committee charters, and company websites. We considered proxies released between June 1, 2017 to October 26, 2018. We looked at the latest definitive proxy filed by a company, including definitive proxy amendments.[7]

We found that within a proxy, and depending on the company, cybersecurity can be mentioned in multiple places and in several different ways using various terms.

In the context of cybersecurity and oversight, we determined: (a) if there was clear disclosure of oversight relating to cybersecurity; (b) if yes, which committee had the oversight; and (c) if there was a dedicated committee created for handling cybersecurity (best in class).

Once it was determined that a company had assigned cybersecurity to a board committee or to general board review, we mapped the members within these committees to their "technology" skill. Technology skill is assigned by MyLogIQ based on an individual director's biography as disclosed in proxies and company websites.

We then determined, based on the number of committee members in each committee with the oversight responsibility, how many directors have technology skill.

For sector analysis, we assigned a top-level sector to correspond with a combination of SIC classifications, NAICS, and investment industry funds which classify companies in their portfolio by sector.

[7] Companies with proxies filed prior to June 1, 2017, companies that are foreign filers, and companies that have not filed as of October 26, 2018 have been excluded from our study. As such, the total eligible companies for the Russell 3000 are 2,830; 1,887 for the Russell 2000; 944 for the Russell 1000; 595 for the S&P 600; 500 for the S&P 500; 396 for the S&P 400; 100 for the S&P 100; and 30 for the Dow 30. The total eligible companies are the basis for this report.

Cyber Risk is a Given; So Is Potential Legal Liability and SEC Enforcement Action

As The Conference Board notes, cybersecurity needs to be seen as an integral piece of everyday business operations and not just as a technology issue.[8]

Cyberattacks are a given. Potential enforcement and liability are also a given. The SEC's February 2018 interpretive guidance and recent commissioner remarks signal that staff are watching.

Understanding a company's top-level organizational approach to cybersecurity helps consumers and investors gauge where accountability rests for privacy protection, legal liability, and continuity of business operations.

What Do the Indices Tell Us?

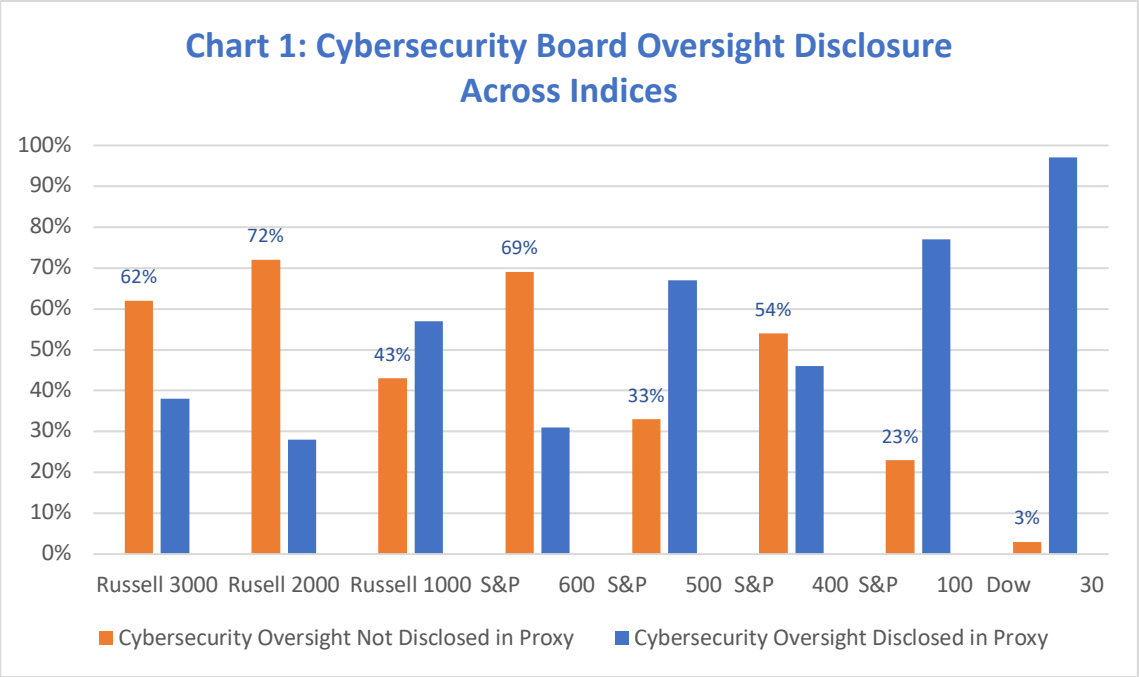
Below is a deeper look at what the eight indices tell us about how companies are responding to cybersecurity concerns at the board level and their risk management structure.

- ***40% or More of the Companies in 5 of the 8 Indices Have Not Disclosed:*** As Chart 1 indicates, board oversight and disclosure of board oversight of cybersecurity varies depending on the index. Less than a third of Russell 2000 companies (528) have disclosed how their boards handle cybersecurity, leaving 1,359 companies that have not. On the other hand, 97% of Dow 30 companies (29) have disclosed how their boards are responding to the cybersecurity threat. Two-thirds of S&P 500 companies (334) have also disclosed what they are doing at the board level. However, this also means that 166 S&P 500 companies have not explained what they are doing.[9]

[8] The Conference Board, 23 Truths About Cybersecurity – Insights from the Cybersecurity Conference: Crucial Collaborations, January 2018

[9] Companies with proxies filed prior to June 1, 2017, companies that are foreign filers, and companies that have not filed as of September 25, 2018 have been excluded from our study. As such, the total eligible companies for the Russell 3000 are 2,830; 1,887 for the Russell 2000; 944 for the Russell 1000; 595 for the S&P 600; 500 for the S&P 500; 396 for the S&P 400; 100 for the S&P 100; and 30 for the Dow 30. The total eligible companies are the basis for this report.

Given that data breaches and shutdowns are an existential threat to today's normal business operations, we find it surprising that companies apparently: a) are not disclosing how their boards manage cybersecurity, or b) have not made cybersecurity a priority for their boards.



- ***Only 11 Cybersecurity Committees:*** As Table 1 below shows, another potential indication that boards have not fully heeded the call to prioritize cybersecurity is that **only 11** companies in the Russell 3000 and only **three** in the S&P 500 have a standalone board committee on cybersecurity.[10] Again, given the nature of the cybersecurity threat, it would appear that more companies need to follow the lead of the companies that do have a dedicated cybersecurity committee.

[10] The three companies with a cybersecurity committee on the S&P 500 also appear on the Russell 3000.

- ***Audit Committees Are Home to Most Cybersecurity Oversight:*** Another key indicator of how US companies are managing cybersecurity at the board level is that a large majority of them place the responsibility with their audit committees. For example, 76% of Dow 30 companies assign cybersecurity to their audit committee.

Table 1: Overview of Key Cybersecurity Indicators in the Dow 30, S&P 500, & Russell 3000*

	Dow 30	S&P 500	Russell 3000
Audit Committee	23	210	598
Full Board Review	2	60	259
Standalone Cybersecurity Committee	0	3	11**
No Cybersecurity Oversight Disclosed[11]	**1**	**166**	**1766**

*Table 2 on p. 10 contains the underlying data for the information in this table.
**Includes the three companies that are also listed on the S&P 500 index.

[11] There is no mention of cybersecurity oversight or related terms in the company's proxy.

A Deeper Look at the Data Disclosed in the Eight Indices

Table 2 below looks at key cybersecurity metrics for all eight indices, including which board committee has responsibility for overseeing cybersecurity risk.

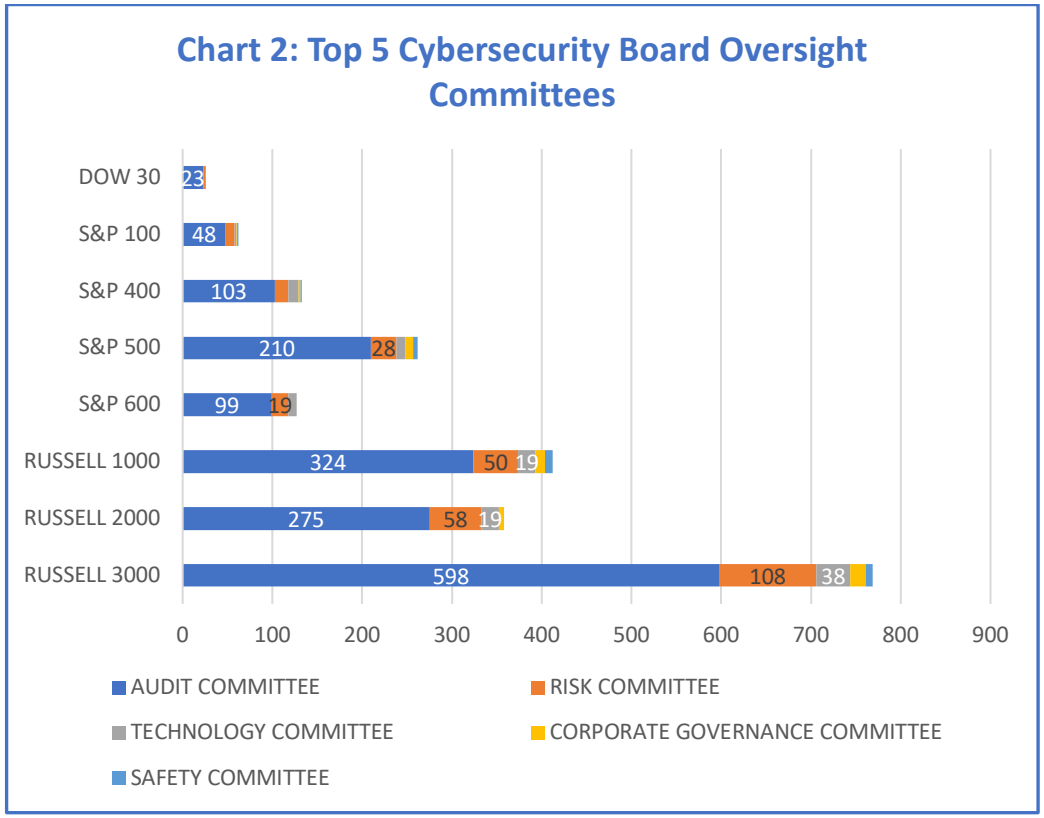
Charts 2-10 below take a deeper look at board committee assignments for cybersecurity within each index.

Table 2: Cybersecurity in the 8 Indices*

	RUSSELL 3000	RUSSELL 2000	RUSSELL 1000	S&P 600	S&P 500	S&P 400	S&P 100	DOW 30
AVERAGE NUMBER OF DIRECTORS ON BOARD	9	9	10	9	11	10	12	12
AVERAGE NUMBER OF DIRECTORS ON BOARD WITH TECHNOLOGY SKILL	3	3	3	3	4	3	5	5
PERCENTAGE OF DIRECTORS WITH TECHNOLOGY SKILL	33%	33%	30%	33%	36%	30%	42%	42%
CYBERSECURITY BOARD OVERSIGHT NOT DISCLOSED IN PROXY	1766	1359	407	413	166	214	23	1
CYBERSECURITY BOARD OVERSIGHT DISCLOSED	1064	528	537	182	334	182	77	29
GENERAL BOARD REVIEW	259	149	110	48	60	44	9	2
CYBERSECURITY COMMITTEE	11	7	4	2	3	2	1	0
TECHNOLOGY COMMITTEE	38	19	19	9	10	11	2	0
SPECIAL COMMITTEE	3	1	2	1	2	0	1	0
RISK COMMITTEE	108	58	50	19	28	15	10	3
SAFETY COMMITTEE	8	0	8	0	5	2	1	0
SECURITY COMMITTEE	4	3	1	1	1	0	1	0
CYEBERSECURITY RELATED SUBCOMMITTE	7	4	3	1	2	1	1	0
AUDIT COMMITTEE	598	275	324	99	210	103	48	23
CORPORATE GOVERNANCE COMMITTEE	17	6	11	0	9	2	1	0
FINANCE COMMITTEE	5	2	3	2	2	0	0	0
COMPLIANCE COMMITTEE	3	3	0	0	0	1	0	0
PUBLIC POLICY COMMITTEE	1	0	1	0	1	0	1	1
QUALITY COMMITTEE	2	1	1	0	1	1	1	0
COMPENSATION COMMITTEE	0	0	0	0	0	0	0	0
EXECUTIVE COMMITTEE	0	0	0	0	0	0	0	0

***Note 1:** Companies with proxies filed prior to June 1, 2017, companies that are foreign filers, and companies that have not filed as of October 26, 2018 have been excluded from our study. As such, the total eligible companies for the Russell 3000 are 2,830; 1,887 for the Russell 2000; 944 for the Russell 1000; 595 for the S&P 600; 500 for the S&P 500; 396 for the S&P 400; 100 for the S&P 100, and 30 for the Dow 30. The total eligible companies are the basis for this report.
Note 2: Some indices are subsets of others or overlap. As such, company totals may not match.
Note 3: Rows 6-21 are a subset of Row 5.

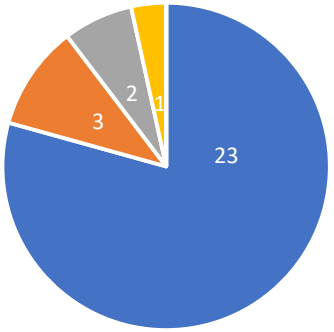
Chart 2 identifies the top five committees tasked with cybersecurity by index. As the data shows, the audit committee is the overwhelming cybersecurity choice for disclosing companies in all eight indices. The risk committee and the technology committee are the second and third choices.



Charts 3-10 below provide detail on which committees have responsibility for overseeing cybersecurity risk for each of the eight indices used in this report. As indicated above, the audit committee is the overwhelming choice for all companies.

As Chart 3 shows, 76% of the Dow 30 disclosing companies place cybersecurity oversight with their audit committees.

Chart 3: Dow 30 Cybersecuirty Oversight by Committee*

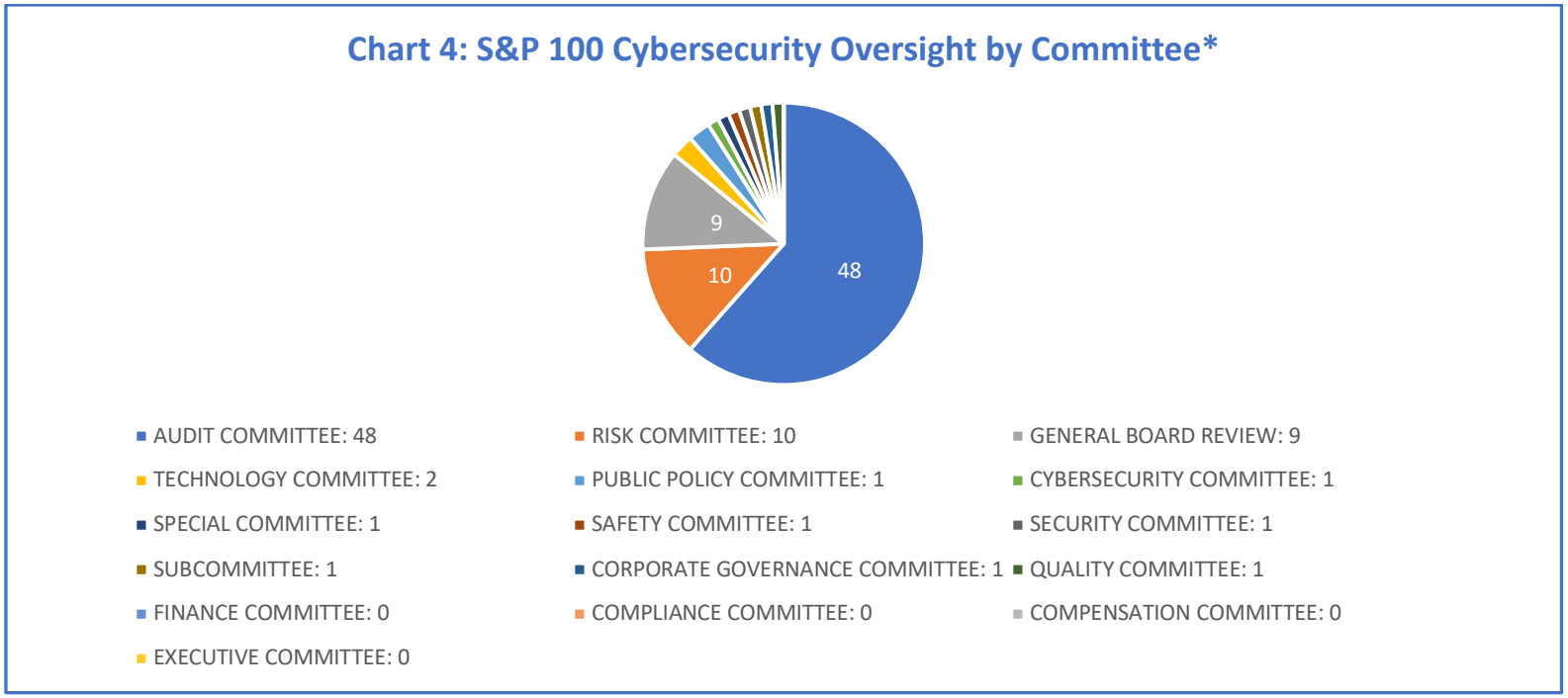


- AUDIT COMMITTEE: 23
- RISK COMMITTEE: 3
- GENERAL BOARD REVIEW: 2
- PUBLIC POLICY COMMITTEE: 1
- CYBERSECURITY COMMITTEE: 0
- TECHNOLOGY COMMITTEE: 0
- SPECIAL COMMITTEE: 0
- SAFETY COMMITTEE: 0
- SECURITY COMMITTEE: 0
- SUBCOMMITTEE: 0
- CORPORATE GOVERNANCE COMMITTEE: 0
- FINANCE COMMITTEE: 0
- COMPLIANCE COMMITTEE: 0
- QUALITY COMMITTEE: 0
- COMPENSATION COMMITTEE: 0
- EXECUTIVE COMMITTEE: 0

*29 S&P 100 companies have disclosed cybersecurity oversight

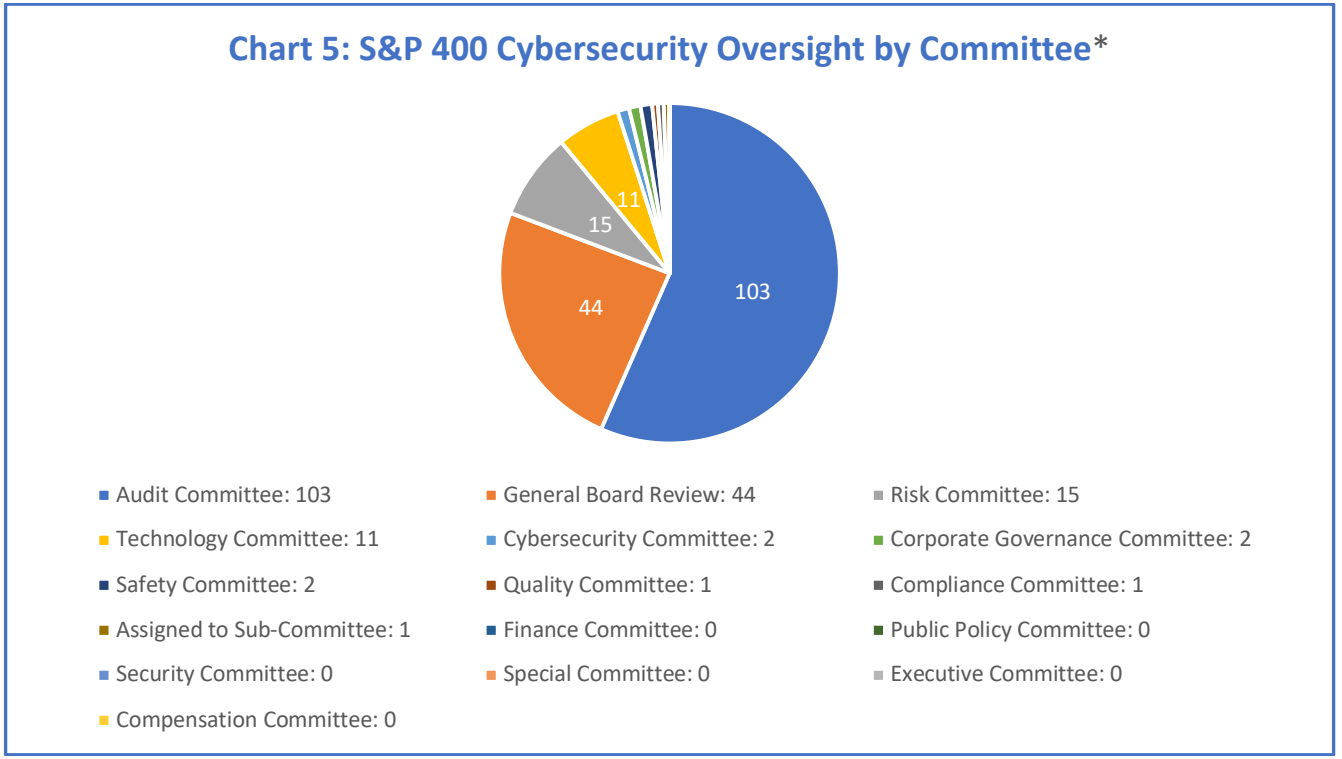
888.564.4910 www.mylogiq.com reports@mylogiq.com

Chart 4 indicates that 61% of the S&P 100 disclosing companies place cybersecurity oversight with their audit committees.



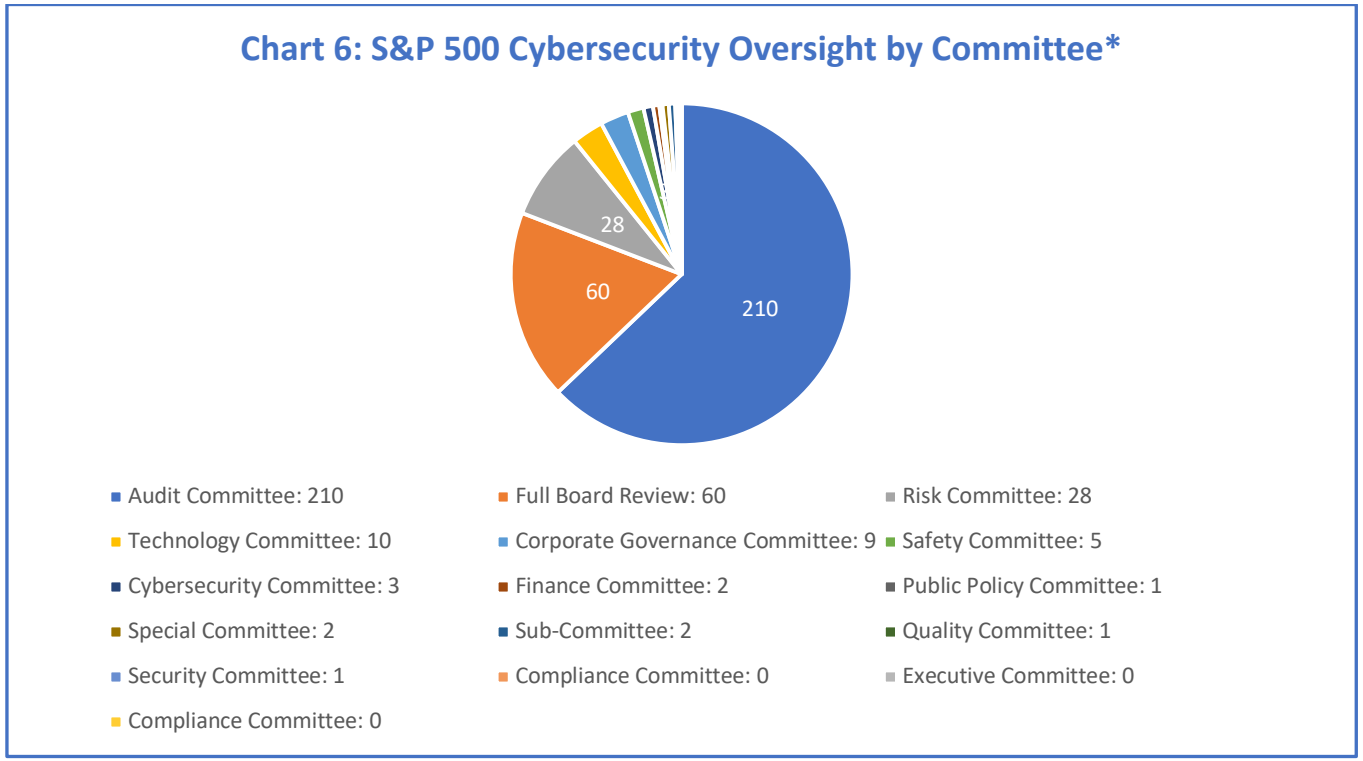
*77 S&P 100 companies have disclosed cybersecurity oversight

As Chart 5 shows, 56% of the S&P 400 disclosing companies place cybersecurity oversight with their audit committees.



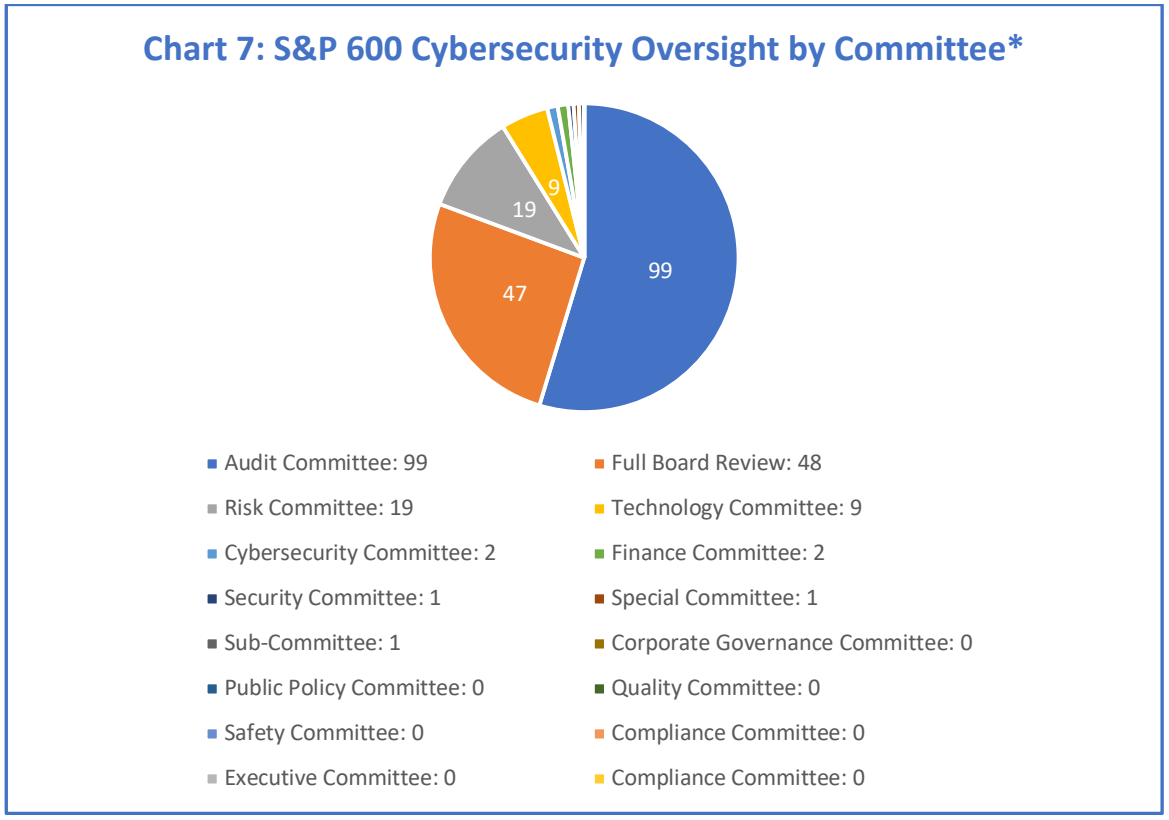
*182 S&P 400 companies have disclosed cybersecurity oversight

Chart 6 shows that 63% of the S&P 500 disclosing companies place cybersecurity oversight with their audit committees.



*334 S&P 500 companies have disclosed cybersecurity oversight

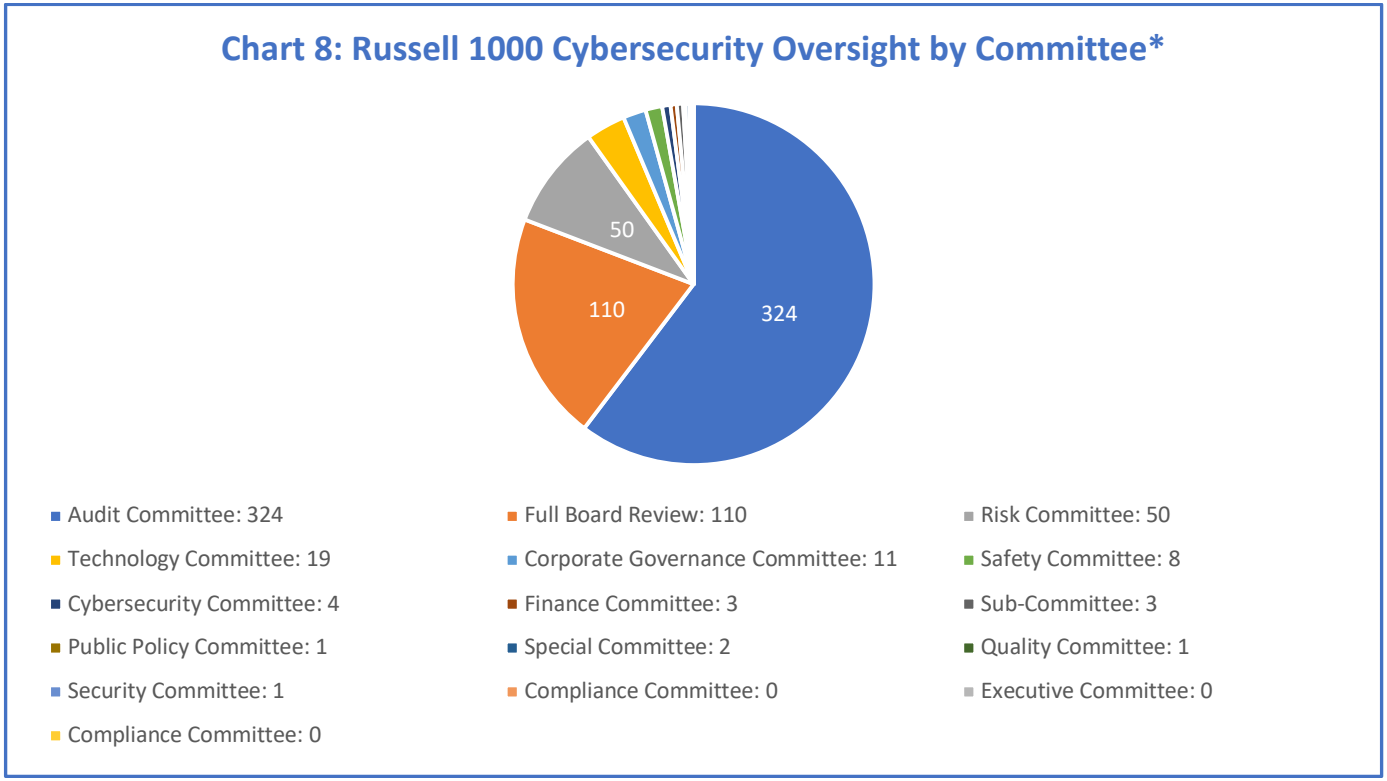
As Chart 7 demonstrates, 54% of the S&P 600 disclosing companies place cybersecurity oversight with their audit committees.



*182 S&P 600 companies have disclosed cybersecurity oversight

888.564.4910 www.mylogiq.com reports@mylogiq.com

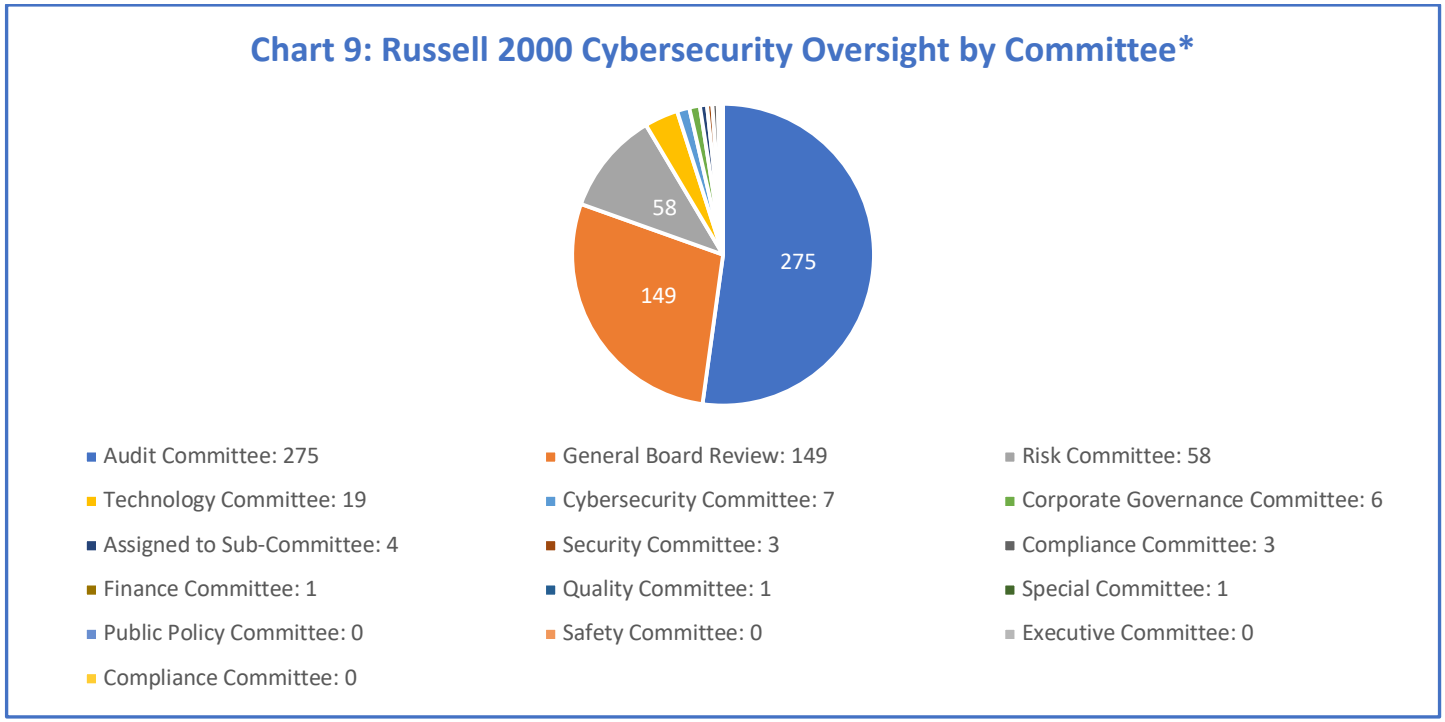
Chart 8 indicates that 61% of Russell 1000 disclosing companies place cybersecurity oversight with their audit committees.



*537 Russell 1000 companies have disclosed cybersecurity oversight

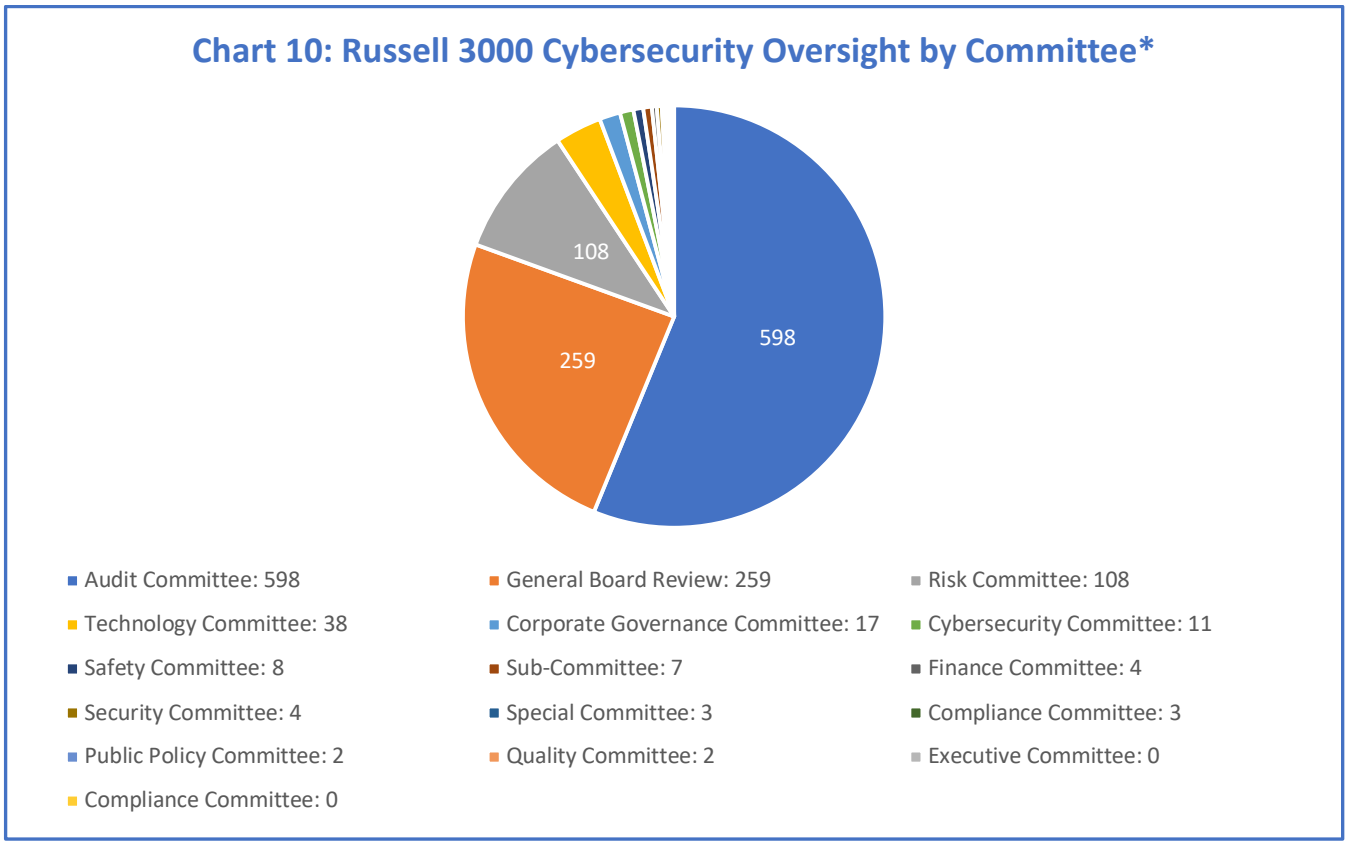
888.564.4910 www.mylogiq.com reports@mylogiq.com

As Chart 9 shows, 52% of the Russell 2000 disclosing companies place cybersecurity oversight with their audit committees.



*528 Russell 2000 companies have disclosed cybersecurity oversight

Lastly, Chart 10 indicates that 56% of the Russell 3000 disclosing companies place cybersecurity oversight with their audit committees.



*1,064 Russell 3000 companies have disclosed cybersecurity oversight

Board Technology Skill

Another potential measure of how a company prioritizes cybersecurity is the technology skill level of its board. Charts 11-13 lay out a range of indicators on technology skill and cybersecurity skill for the eight indices in this report.

Chart 11 identifies the average number of board members with a technology background for each index. On the upper end, the Dow 30 and the S&P 100 average five members with technology experience. On the lower end are the four indices that average three members.

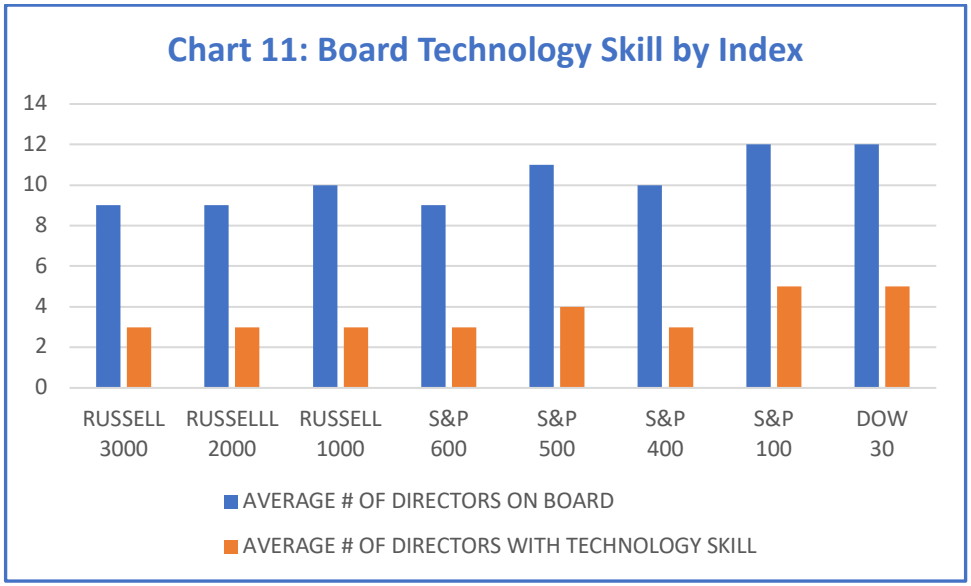


Chart 12 displays cybersecurity skill, with the S&P 100 leading with an average of two directors per company with a cybersecurity background. The remaining seven indices average one cybersecurity director per company.

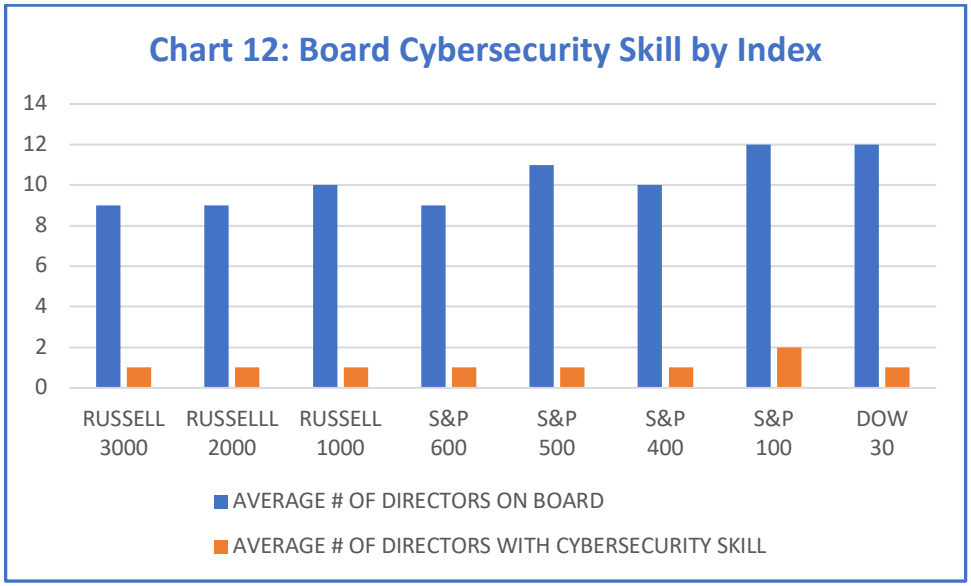
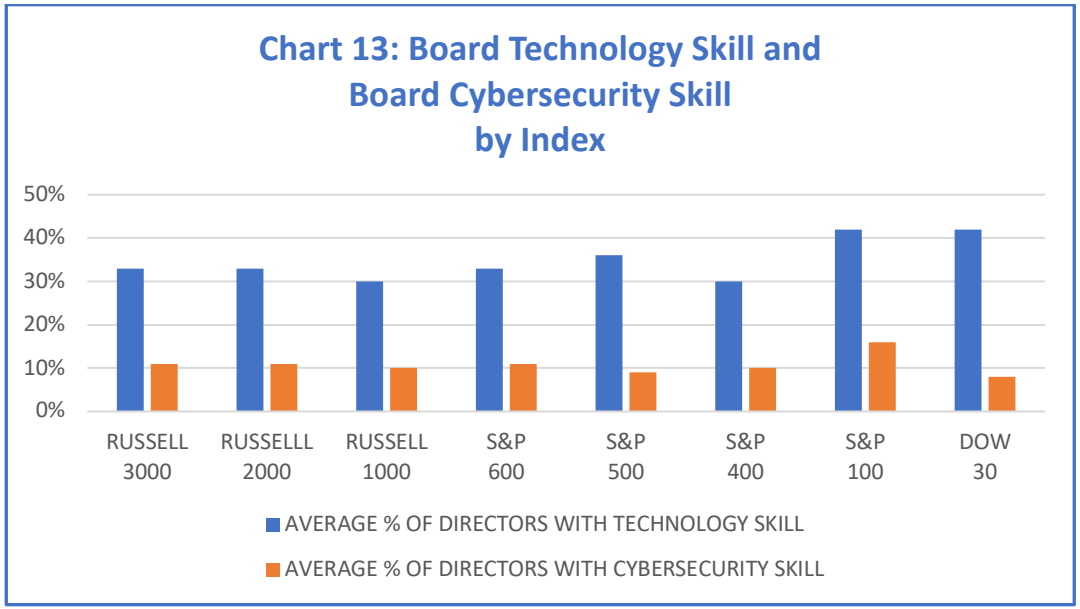


Chart 13 presents both the average percentage of directors with technology skill and those with cybersecurity skill for the eight indices.



Cybersecurity Overview in the S&P 500

We take a deeper look at cybersecurity in the S&P 500. Here are some of our findings.

- More than a third of S&P 500 companies, 172, do not mention cybersecurity oversight in their latest proxy reports.
- 11% of companies indicate that their board has general responsibility for cybersecurity.
- Nearly two-thirds of the 328 companies that have disclosed that their board is responsible for cybersecurity through a board level committee or subcommittee task that oversight to their audit committee.
- Only 24% of S&P 500 companies have disclosed that they have at least one director with cybersecurity skill.
- Table 3 below has the details.

Table 3: S&P 500 Cybersecurity Disclosure & Board Oversight

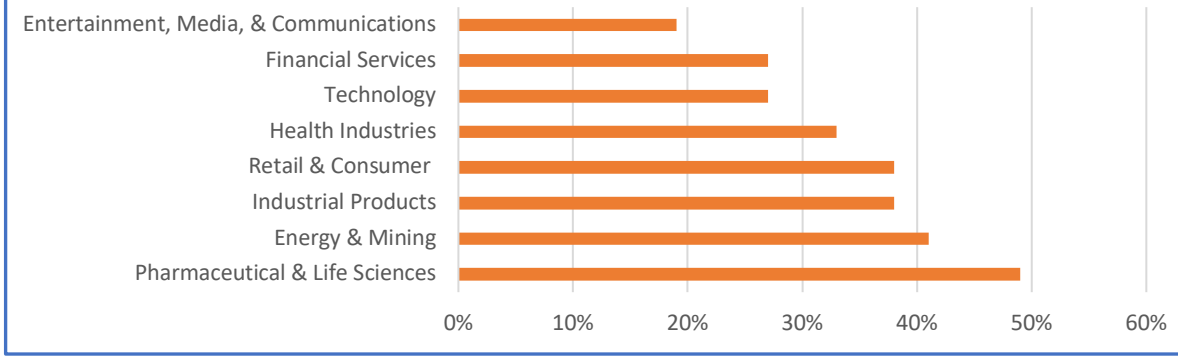
	COMPANY COUNT	PERCENTAGE OF ALL 500 COMPANIES
NO CYBERSECURITY DISCLOSURE*	166	33%
FULL BOARD REVIEW	60	12%
CYBERSECURITY COMMITTEE	3	1%
TECHNOLOGY COMMITTEE	10	2%
SPECIAL COMMITTEE	2	<1%
SUB-COMMITTEE	2	<1%
AUDIT COMMITTEE	210	42%
RISK COMMITTEE	28	5%
CORPORATE GOVERNANCE COMMITTEE	9	2%
SAFETY COMMITTEE	5	1%
FINANCE COMMITTEE	2	<1%
PUBLIC POLICY COMMITTEE	1	<1%
SECURITY COMMITTEE	1	<1%
QUALITY COMMITTEE	1	<1%
TOTAL	500	100%

*There is no mention regarding oversight of cybersecurity or related terms in the company's proxy.

Sector Analysis of Cybersecurity Among the S&P 500

- Pharmaceutical and life sciences companies in the S&P 500 lead the sectors, in percentage terms, that do not mention the word cyber or related words in their 2017 proxies.
- Interestingly, close to a third of S&P 500 technology companies also did not disclose on cyber or related terms.
- Chart 14 below has the details.

Chart 14: Percentage of S&P 500 Companies by Sector That Have Not Disclosed Cyberseurity Oversight



S&P 500 Companies Distribution of Cybersecurity Responsibility Among Board Committees by Sector

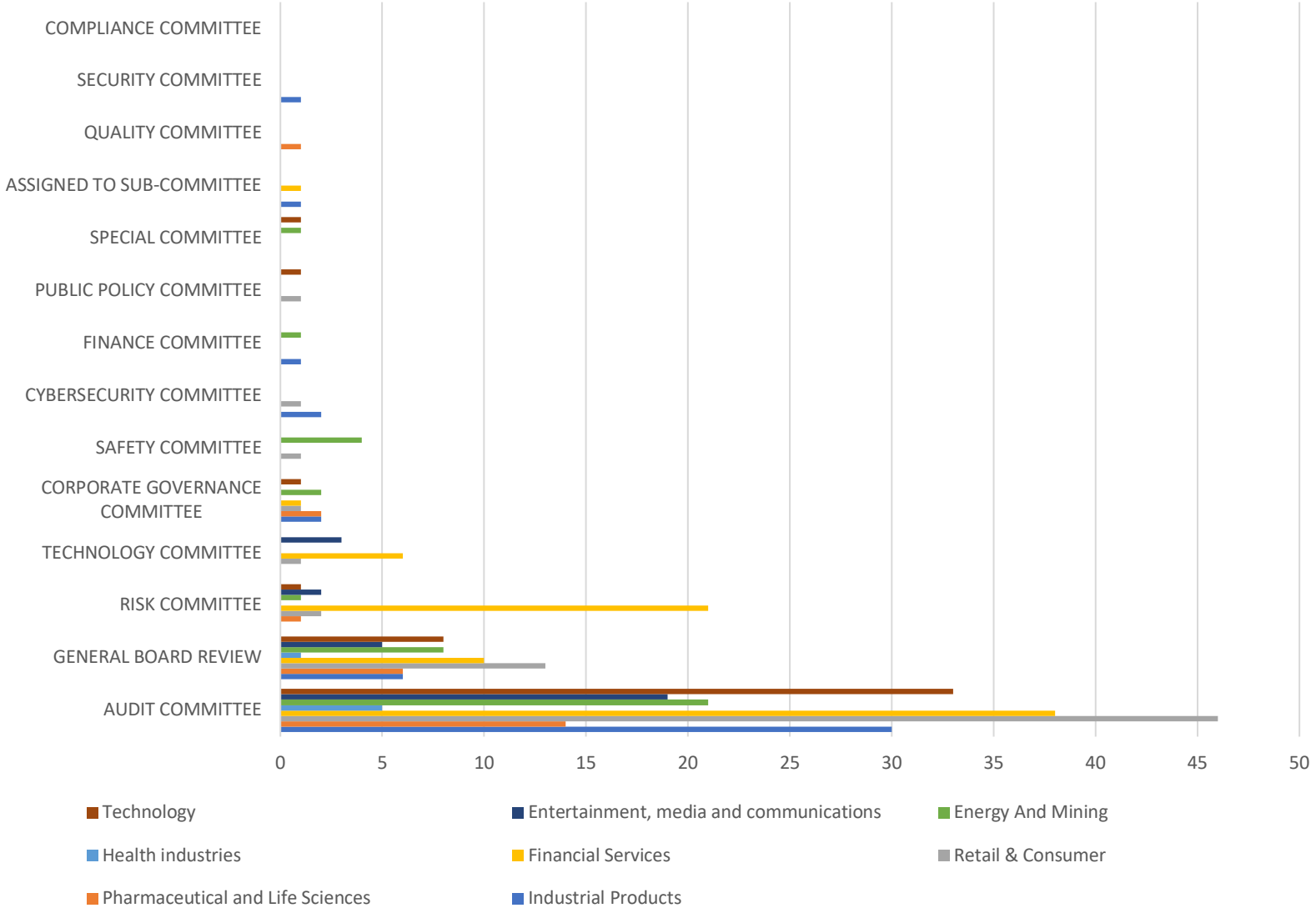
- As mentioned above, of the 334 S&P 500 companies that indicate a board responsibility for cybersecurity, 63% place that responsibility with the audit committee.
- All eight sectors show an overwhelming preference for their boards' audit committees to be vested with this responsibility.
- The second most frequent assignment was the risk committee with 9% of the 328 cybersecurity disclosing companies choosing this committee.
- Table 4 and Chart 15 below have the details.

Table 4: Sector Analysis of Board Committee Responsibility for Cybersecurity in the S&P 500*

Sector	Audit	General Board Review	Risk	Technology	Sub-committee	Corporate Governance	Safety	Cyber-security	Finance	Public Policy	Security	Quality	Special
Retail & Consumer (n=66)	48	13	2	1	0	1	1	1	0	1	0	0	0
Financial Services (n=77)	38	10	21	6	1	1	0	0	0	0	0	0	0
Industrial Products (n=43)	30	6	0	0	1	2	0	2	1	0	1	0	0
Energy & Mining (n=38)	21	8	1	0	0	2	4	0	1	0	0	0	1
Technology (n=45)	33	8	1	0	0	1	0	0	0	1	0	0	1
Entertainment, Media, & Communications (n=29)	21	5	2	3	0	0	0	0	0	0	0	0	0
Health Industries (n=6)	5	1	0	0	0	0	0	0	0	0	0	0	0
Pharmaceutical & Life Sciences (n=24)	16	6	1	0	0	2	0	0	0	0	0	1	0
TOTAL	206	57	28	10	2	9	5	3	2	2	1	1	2

*334 S&P 500 companies have disclosed cybersecurity board oversight.

Chart 15: S&P 500 Sector Analysis of Cybersecurity Oversight by Committee



About

Multidimensional Public Company Intelligence · Simple · Proactive · Comprehensive

MyLogIQ offers an unrivaled AI-augmented public company intelligence solution with CompanyIQ™.

- **CompanyIQ™:** Content, analytics, and predictive engine built with intelligence from more than 1.5 million SEC filings over the last twenty years.
    - **Shareholder Engagement, Proposals, & No-Action Letters.**
    - **Executive Compensation.**
    - **Director Compensation.**
    - **Corporate Governance, Charters, & Policies.**
    - **SEC Comment Letters.**
    - **SEC Disclosures.**
    - **Trends in Risk Factors, MD&A, Earnings Releases.**
    - **Detailed Financials.**
    - **Audit Fees & SOX Analysis.**

For more details, visit us at www.mylogiq.com or contact info@mylogiq.com or 888-564-4910.

For Press Inquiries and details: Contact Ganesh Rajappan, 415.378.2987

Reports You May Be Interested In

- To subscribe to reports and analytics, email info@mylogiq.com or call 888-564-4910.

Disclosures:

1) Risk Factors and Leading Concerns
2) How Efficient Are Company Disclosures in Their Ks and Qs, and What Has the Season Taught Us?
3) Benchmarking Financial Footnotes in Annual and Quarterly Filings
4) Changes in MD&A Discussion
5) Non-GAAP Disclosures and Compliance
6) What Has Been the SEC's Focus on Comments?
7) ASC 842 Lease Commitments, Early Adopters Trend

Corporate Governance:

1) Director Gender and Diversity
2) Are You an Independent Board Member If You Serve More Than 10-15 Years?
3) How Much Does a Board of Director Earn Per Meeting?
4) Analysis of Shareholder Proposals and Leading Trends
5) Risk Oversight and Cybersecurity and Company Boards - Who Is Responsible?

Executive Compensation:

1) CEO Pay Ratio - S&P 500 and Russell 3000 - How Long Does a CEO Work to Earn a Median Employee's Annual Pay?
2) What Is the CFO Pay-Ratio and How Does It Compare with the CEO Pay-Ratio?
3) Pay Elements of CEO and CFO Compensation Across Large Cap, Mid-Cap and Small-Cap Companies