Diligent Institute | BITSIGHT

Cybersecurity, audit, and the board:

How does board oversight impact cybersecurity performance?

March 2024

Diligent Institute | BITSIGHT

About Diligent Institute

Diligent Institute informs, educates, and connects leaders to champion governance excellence. We provide original, cutting-edge research on the most pressing issues in corporate governance, certifications and educational programs that equip leaders with the knowledge and credentials needed to guide their organizations through existential challenges, and peer networks that convene directors and corporate executives to share best practices and insights.

Learn more at diligentinstitute.com

About Bitsight

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

Learn more at bitsight.com

Diligent Institute | BITSIGHT

Contents

Introduction

The rapid escalation in the frequency and severity of cyber incidents has positioned cyber risk as one of the foremost challenges confronting boards.[1] With cyber threats becoming increasingly sophisticated and pervasive, boards are under mounting pressure to effectively address cybersecurity risks to safeguard their organizations' interests. With projected financial losses from data breaches estimated to reach approximately USD 10.5 trillion by 2025, and new pressure from regulators like the SEC, the oversight role of the board becomes even more crucial.[2]

Boards are prioritizing robust oversight mechanisms to mitigate cyber risk and protect their organizations' financial health and reputation in an ever-evolving digital world. However, the approaches boards take to address cyber risk vary, prompting questions about the effectiveness of different board governance structures and strategies.

Diligent Institute and Bitsight, recognizing the need for deeper insight into board practices regarding cybersecurity oversight and the impact they have on organizations, set out to better understand how boards are addressing cyber risks and the outcomes of these approaches. Through this report, we aim to shed light on several key questions:

- *Is there a relationship between cybersecurity performance and financial performance?*
- *Do companies demonstrate better performance in cybersecurity when specialized committees are established for oversight, versus assigning cyber risk oversight to the audit committee?*
- *Does audit committee oversight of cyber risk correlate with security performance?*
- *Does the presence of cyber experts on boards correlate with security performance?*
- *What else might we learn about cyber risk governance from companies that have high security performance ratings?*

By addressing these questions, we aim to provide actionable insights that can inform best practices in corporate governance and enhance the structural oversight of cyber risk.

1. Corporate Board Member, Diligent Institute, BDO, What Directors Think, January 2024.
2. NightDragon, Diligent Institute, State of Cyber Awareness in the Boardroom, September 2023.

Methodology

Our analysis consists of publicly-available data on 4,149 mid to large-cap companies in public indices across Australia, Canada, France, Germany, Japan, the United Kingdom, and the United States. Leveraging board data sourced from Diligent Market Intelligence in late November 2023, we examined the board structures and director skillset backgrounds of these companies.

We then identified companies with specialized board committees dedicated to cyber, risk, or safety oversight. Throughout this report, we collectively referred to these committees as "specialized risk committees."

We have also categorized cybersecurity oversight at the committee level into three groups to assess their potential impact on cybersecurity risk ratings:

1. Companies with a specialized risk committee to oversee cybersecurity.
2. Companies without a specialized risk committee, where we have made the assumption that the audit committee has been tasked with overseeing cybersecurity risk along with other areas of enterprise risk.
3. Companies with neither an audit nor a specialized risk committee, where we have made the assumption risk is overseen at the full board level.

For the purposes of this report, we have classified directors as "cybersecurity experts" if they meet the following criteria:

- They are current or former Chief Information Security Officers (CISOs), or
- They are current or former CEOs, Chief Information Officers (CIOs) or Chief Technology Officers (CTOs) of a cybersecurity company.

We also have correlated each company's cyber oversight structure with their corresponding security performance data, obtained from Bitsight. The correlation method involved averaging the ratings within each category to identify discernible patterns. Bitsight creates cybersecurity ratings based on externally observable measurements of an organization's security posture. The data was pulled between December 2023 and February 2024 and the ratings range from 250 to 900 (in 10-point increments), grouped into three broad classifications:

1. Basic Security Performance: A rating ranging from 250 to 630 comprising 12% of our sample.
2. Intermediate Security Performance: A rating ranging from 640 to 730 comprising 47% of our sample.
3. Advanced Security Performance: A rating ranging from 740 to 900 comprising 41% of our sample.

A more detailed breakdown of the factors that inform this rating can be found in the Appendix.

Key findings

Companies with advanced security ratings create nearly four times the amount of value for shareholders as companies with basic security ratings. On average, the Total Shareholders' Return (TSR) over three and five years for companies in the advanced security performance range is approximately 372% and 91% higher, respectively, than their peers in the basic security performance range.

Companies with a specialized risk or audit committee had higher security performance ratings on average. Companies falling within these two categories have an average security rating of 710, whereas companies lacking both committees have an average security rating of 650. The findings also suggest that the distribution of security ratings among companies with specialized risk and audit committees tends to skew towards the advanced security performance range, whereas companies lacking either of these committees tend to skew towards the basic security performance range.

Having a cybersecurity expert on the board is not enough. Integrating a cybersecurity expert into the board committee tasked with cybersecurity risk oversight makes a significant difference in an organization's performance. Merely having a cybersecurity expert on the board does not correlate to having a higher security performance rating. Companies with cybersecurity experts on either audit committees or specialized risk committees achieve an average security performance rating of 700, whereas companies with cybersecurity experts but not on either committee attain a security rating of 580. Regardless of this, the percentage of companies with cyber experts on the board remains significantly low. Only 5% of companies within the sample had cyber experts on their boards.

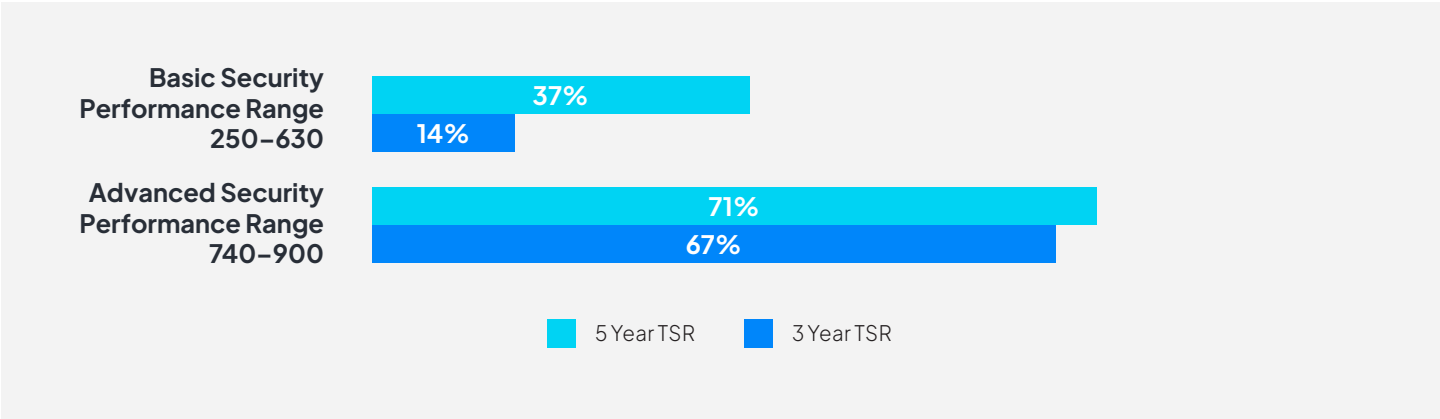
Highly regulated industries tend to outperform other industries in terms of cybersecurity performance. Of the companies with advanced-level security performance ratings, a full third (33%) came from the financial services sector – with an average rating of 720. The sector with the highest average rating overall though, was healthcare at 730. By comparison, nearly a quarter (24%) of companies with basic security performance ratings came from the industrials sector, and the sector with the lowest overall performance rating was the communications sector, at 630.

Security rating and financial performance

Companies with advanced security ratings create nearly four times the amount of value for shareholders as companies with basic security ratings.

Our analysis reveals that companies with superior security performance also demonstrate notably higher financial performance compared to those in the basic security range. Over a three-year period, the average total shareholder return (TSR) for companies with advanced security performance ratings was 67%, compared to 14% for companies with basic ratings. Similarly, measured over a longer duration of five years, companies in the advanced performance range exhibit an average TSR of 71%, while those in the basic performance range have an average TSR of 37%.

Why do companies with higher cybersecurity scores perform better financially? There are several possible explanations. Some of the companies with high cybersecurity scores are in high-growth sectors, such as technology, that have had strong financial performance over the last several years. Additionally, the improved performance may also stem from the fact that companies in the advanced security performance bracket also possess robust governance fundamentals. According to our analysis, approximately 76% of directors on the boards of these companies are independent. In contrast, for companies in the basic security performance category, this figure decreases to about 66%.

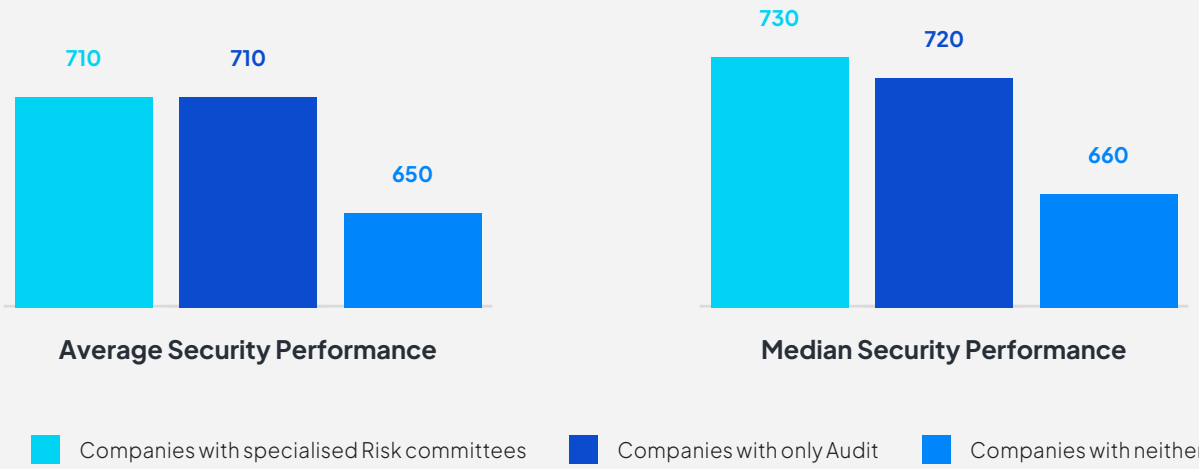


Board structure and security rating

Our research indicates that companies with both specialized risk committees and audit committees tend to achieve higher average security ratings compared to those with neither, at 710 and 650 respectively.

Furthermore, the median security rating for companies with specialized committees stands at 730, which decreases to 720 for companies with just audit committees. By contrast, companies lacking both types of committees experience a notable decrease in their median security performance rating, at 660.

Average and median security performance ratings

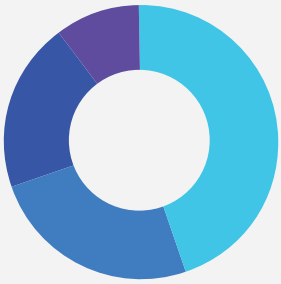


Looking more closely at the distribution of security performance ratings, the data once again reveals a positive correlation between the presence of audit and specialized risk committees (focused on risk, cyber, and safety) and cybersecurity performance ratings. The data indicates that for companies lacking either committee, their rating distribution skews towards the lower end of the intermediate and basic rating ranges. Roughly 72% of companies without either committee fall within this range. By contrast, for companies with specialized risk committees and audit committees only, this percentage drops to 30% and 33% respectively.

Among the companies in our sample with specialized risk committees (n=1,065), 45% demonstrate advanced security performance. Similarly, among the companies with Audit committees (n=2888), 41% exhibit advanced security performance. However, for companies lacking both committees (n=196), only 16% achieve advanced security performance.

Distribution of security performance scores:

Companies with specialized risk committees



45%	Advanced Security Performance Range 740–900
25%	Intermediate Security Performance Upper Range 700–730
20%	Intermediate Security Performance Lower Range 640–690
10%	Basic Security Performance Range 250–630

Companies with only audit committees

41%	Advanced Security Performance Range 740–900
26%	Intermediate Security Performance Upper Range 700–730
22%	Intermediate Security Performance Lower Range 640–690
11%	Basic Security Performance Range 250–630

Companies with neither risk nor audit committees

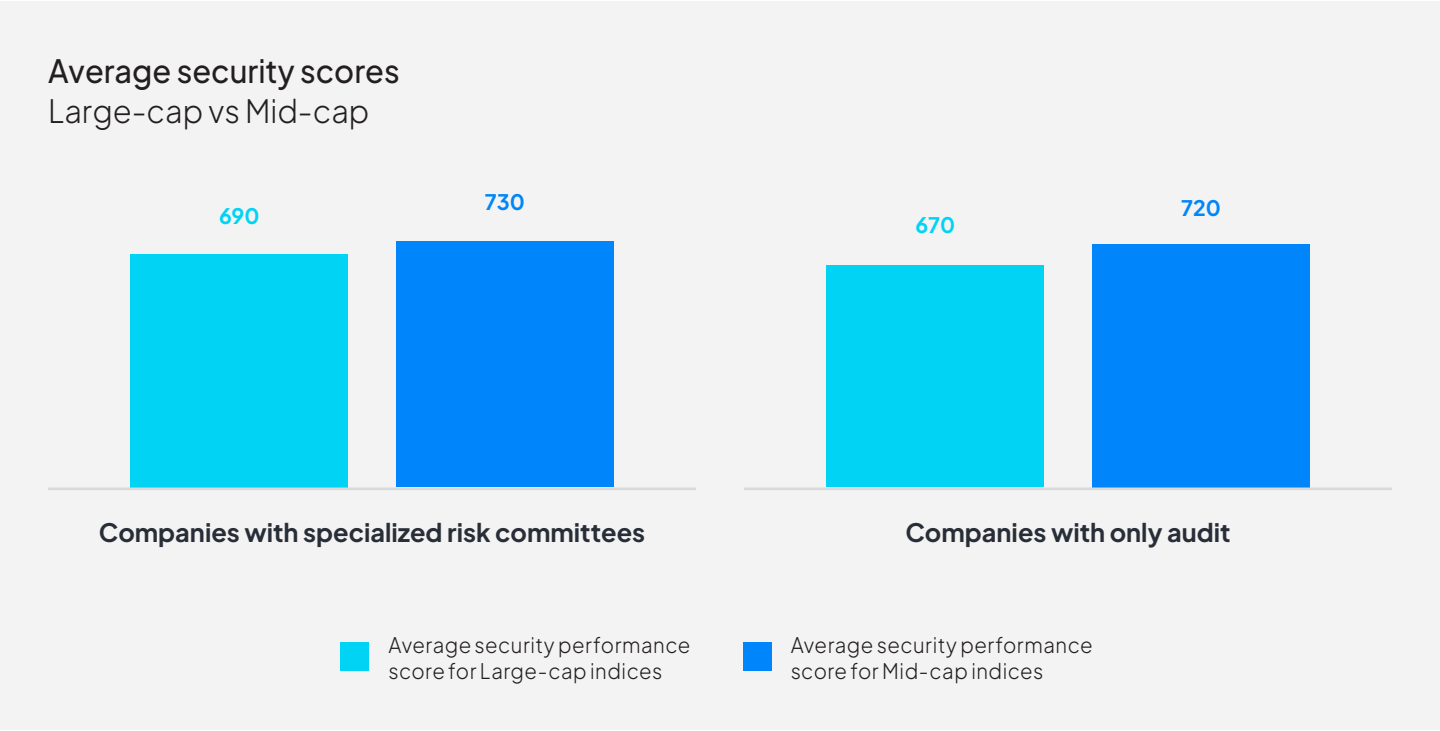
16%	Advanced Security Performance Range 740–900
12%	Intermediate Security Performance Upper Range 700–730
35%	Intermediate Security Performance Lower Range 640–690
37%	Basic Security Performance Range 250–630

Why would having a board committee dedicated to overseeing cyber risk produce better cybersecurity performance? One possible explanation is that delegating oversight of complex areas of risk – like cyber – allows for more detailed focus by select members of the board. Committees are better positioned to dive deep into specific cybersecurity issues and they can develop stronger relationships with the executives charged with the day-to-day cybersecurity operations. This, in turn, can lead to better cybersecurity-related policy, budget and other decisions being made at the board level.

Security rating and market capitalization

Our findings indicate that across the countries we analyzed, the mid-cap indices have higher average security ratings compared to the large-cap indices. The data reveals that large-cap index companies with specialized risk committees have an average security rating of 690, whereas mid-cap companies with specialized risk committees demonstrate have an average rating of 730. Similarly, among companies with only audit committees, those in the mid-cap indices have an average security rating of 720, surpassing their counterparts in the large-cap indices at 670.

One factor that may contribute to this disparity is the size of the attack surface of mid-cap and large-cap companies. Large-cap companies on average leverage significantly more technology assets than mid-cap companies; they tend to employ more people, have larger operations to run, and can be more geographically dispersed. More technology assets mean they have a larger attack surface to defend. Despite being well-resourced, larger organizations still face significant challenges defending a larger attack surface compared with smaller companies.



Cybersecurity experts on boards

In joint research from Diligent Institute and NightDragon, we discovered that the presence of cyber experts on the boards of S&P 500 companies is relatively low, with only 12% of companies having a member with cyber expertise.[3]

While the inclusion of cyber experts on boards is commendable and encouraged, it is essential to recognize that their presence alone may not directly improve cybersecurity performance. Our research suggests that there is no significant correlation between the presence of cyber experts on boards and cybersecurity performance ratings. However, when these experts are integrated into existing structures such as the committees that oversee cyber, a notable correlation with security performance emerges.

We identified two companies where cyber experts were present, yet neither had specialized committees nor audit committees. Interestingly, for these companies, their counterparts' cybersecurity ratings were on average 21% higher. This observation suggests that the emphasis may lie more on structural frameworks combined with individual expertise when it comes to enhancing cybersecurity performance.

Companies seeking to hire cybersecurity expertise for the board should first ensure that the board is appropriately organized so that expertise can be properly incorporated into the oversight mechanisms.

Average security performance

700

Companies with cyber expert on the audit or specialized risk committee

580

Companies with cyber expert not on the audit or specialized risk committee

3. Diligent Institute, NightDragon, State of Cyber Awareness in the Boardroom, September 2023.

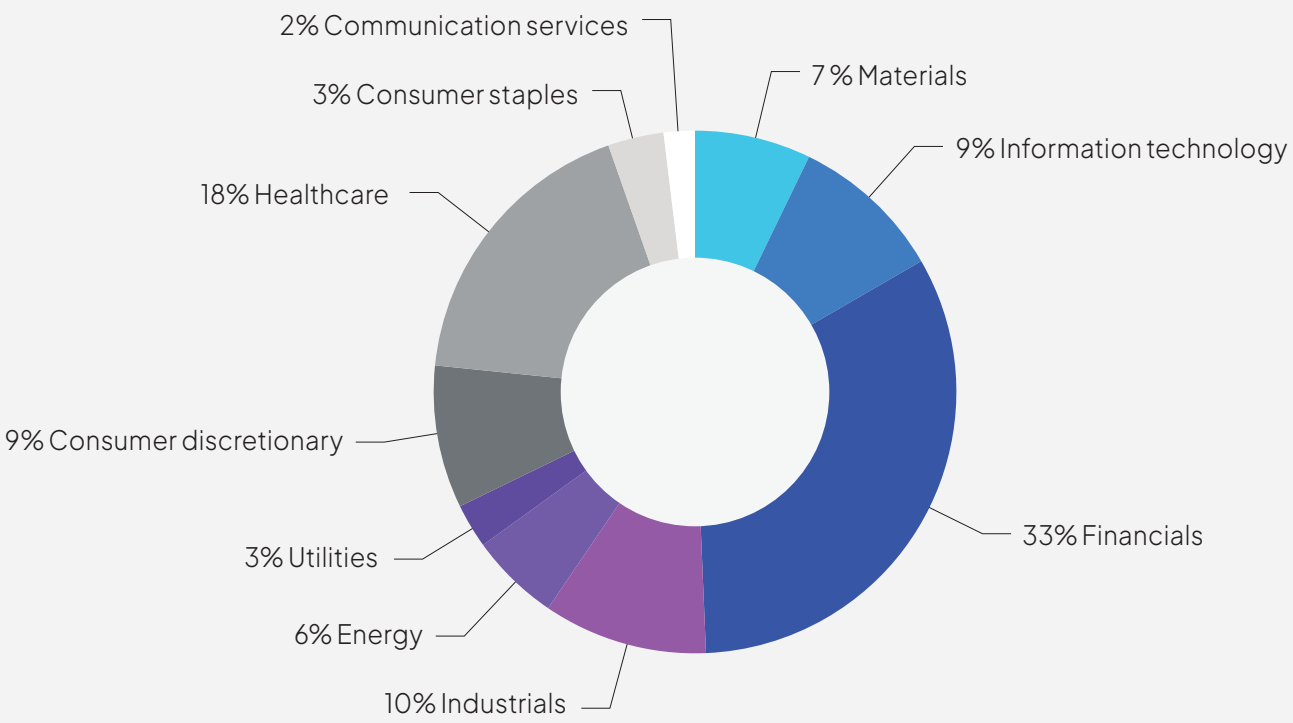
Security rating by sector

Looking at the demographics of the companies in each security rating range, we see that the financial sector makes up about one-third (33%) of all companies in the advanced performance range, likely due to strict cybersecurity regulation in this industry.

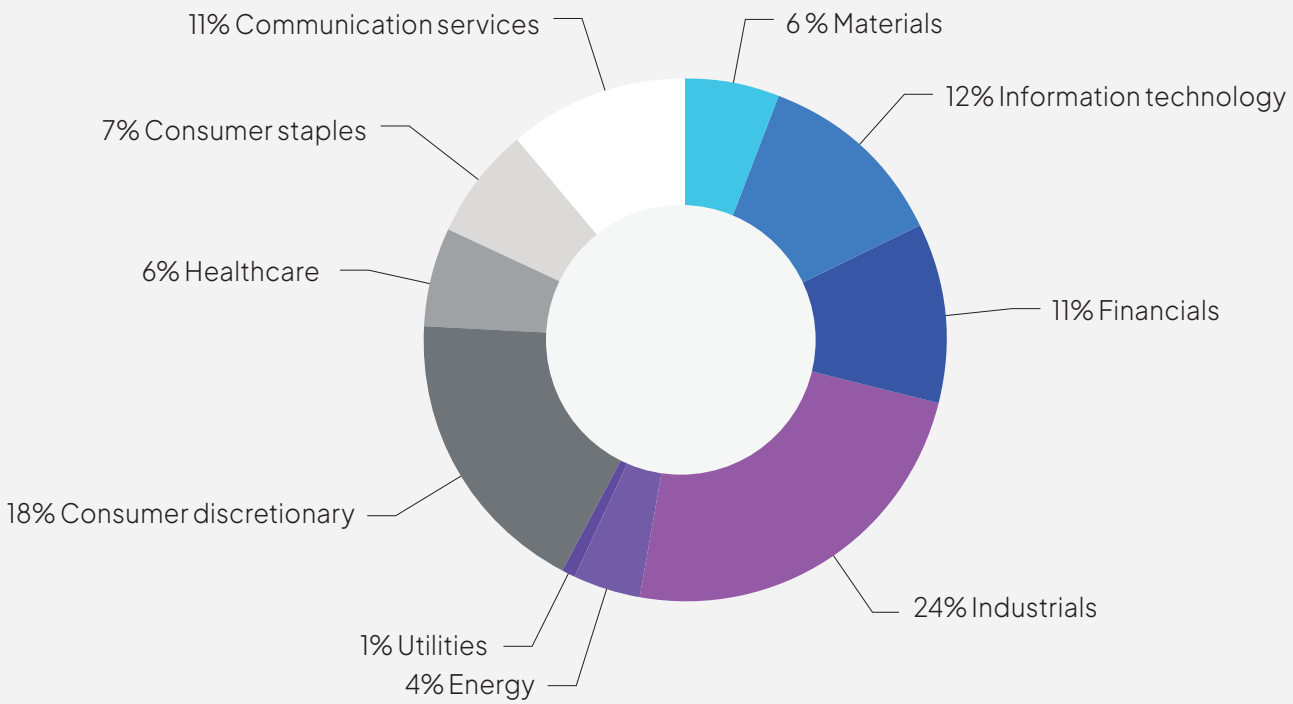
Conversely, among companies categorized within the basic security performance range, those in the industrials sector account for nearly a quarter, while the financial sector accounts for approximately 11%. Overall, companies within the healthcare sector have the highest average security rating of all industry groups analyzed, at 730. The sector with the lowest average security rating is the communication services sector at 630.

It is important for boards to benchmark their organization's cybersecurity performance with peers or across entire sectors and industries on an ongoing basis. This type of benchmarking helps boards know how their company's programs are performing over time and whether that performance is aligned with industry standards of care. In light of the SEC regulations around cybersecurity disclosure, more companies are disclosing benchmarking data to communicate cybersecurity performance to shareholders and the broader marketplace.

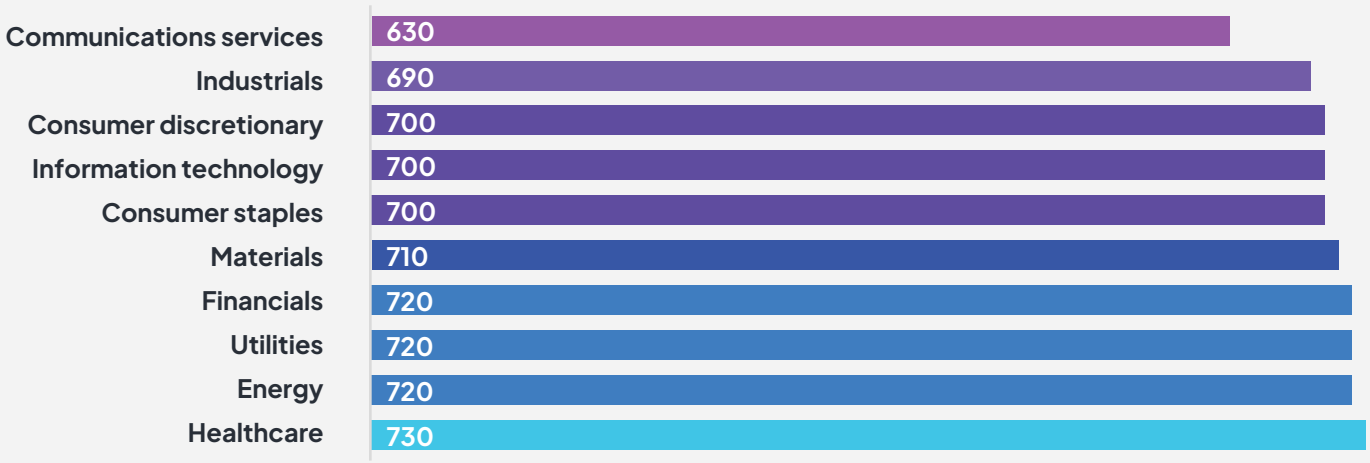
Sector breakdown of companies in the advanced security performance range



Sector breakdown of companies in the basic security performance range



Average security performance rating by sector



Regional differences in board structures and cybersecurity oversight

Establishing specialized committees to supervise risks like cyber is advised by numerous regulatory mandates. Nonetheless, our analysis indicates that the prevalence of such risk committees varies significantly across different countries. In Australia's ASX 300, 90% of the analyzed companies had at least one or more specialized committees of this nature. In stark contrast, within Japan's Nikkei 225 index, only 3% of companies had such specialized committees.

Percent of companies with specialized risk committees
Breakdown by country

Australia	United Kingdom	Canada	France	United States	Germany	Japan
90%	48%	45%	38%	17%	17%	3%

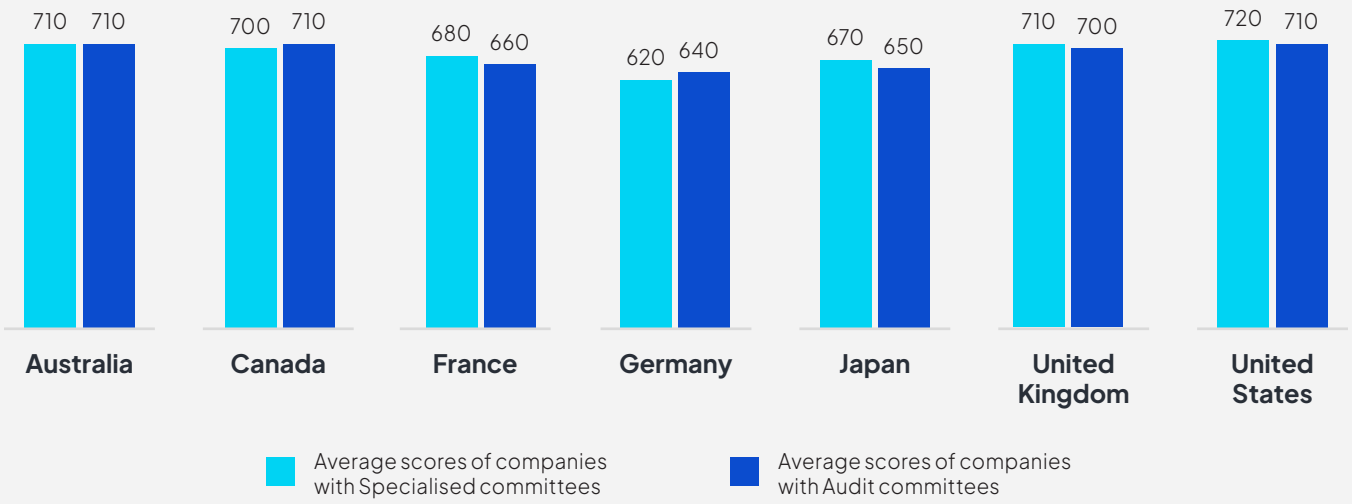
Our findings also indicate that France exhibits a relatively higher presence of cyber experts on their boards compared to the indices analyzed in other countries. In France's CAC 40 Index, for instance, four companies have cyber experts on their boards, representing approximately 10% of the companies within the index. While this number may seem modest, it is notable when contrasted with the United States' Russell 3000, where we identified approximately 205 companies with cyber experts, accounting for 6% of the index's companies. Conversely, countries such as Japan, Australia, and Canada have relatively fewer cyber experts on their boards, ranging from 1% to 2%.

In Australia, Canada, the United Kingdom, and the United States, companies with specialized and audit committees typically demonstrate higher average cyber ratings compared to some of the other countries in our analysis ranging from approximately 700 to 710. Conversely, companies in Japan with specialized committees exhibit the lowest average security rating relative to other countries in our sample at 670.

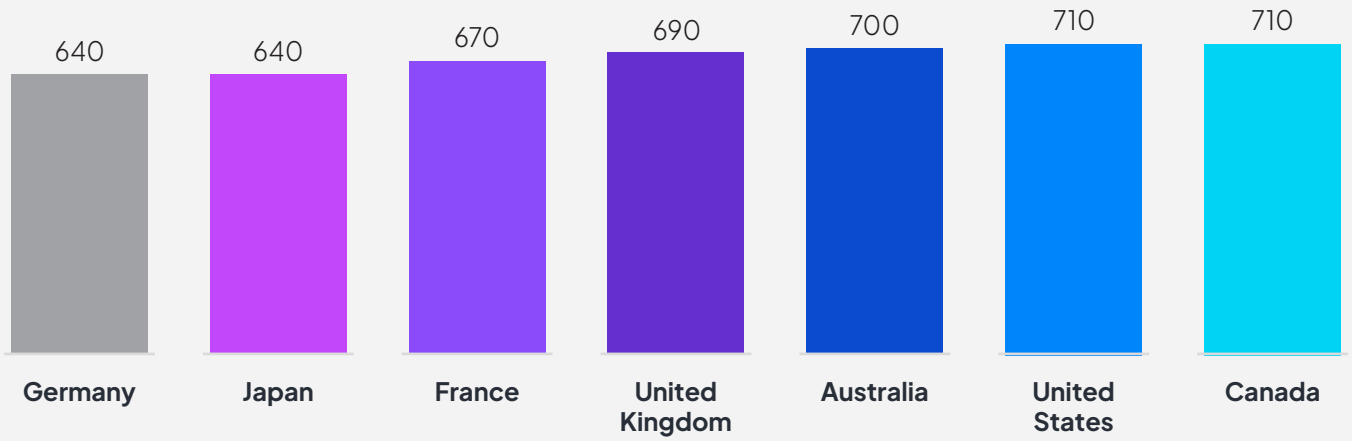
Percentage of companies with a cyber expert on the board

France	United States	Germany	United Kingdom	Japan	Australia	Canada
10%	6%	5%	3%	2%	1%	1%

Average security performance score
Breakdown by country



Average security rating per country



Appendix

Bitsight's security rating measures cybersecurity performance over time – an organization's effectiveness in preventing cybersecurity incidents. According to independent studies, the Bitsight rating has significant, clear correlation with critical outcomes, including cybersecurity incidents, ransomware attacks, and company financial performance. For a detailed methodology, visit www.bitsight.com/security-ratings/trusted-ratings.

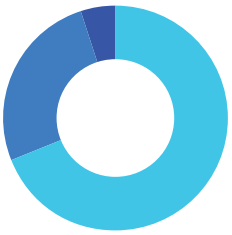
Bitsight continuously collects cybersecurity data across 23 risk vectors to measure cybersecurity performance:

- **Botnet infections:** Devices on a company's network were observed participating in botnets as either bots or Command and Control servers. Botnets can be used to exfiltrate corporate secrets and sensitive customer information, repurpose company resources for illegal activities, and serve as conduits for other infections.
- **Potentially exploited systems:** Devices observed to be running potentially malicious or unwanted software; e.g. greyware or adware. These events are often indicative of other infections, and, like botnet infections, reflect insufficient device controls.
- **Unsolicited communications:** Systems observed to be scanning other hosts in patterns that are typical of malware seeking new hosts to infect.
- **Spam propagation:** Systems that have been used to propagate spam email (which is a common cybercriminal use for compromised machines).
- **Malware servers:** Servers that are hosting malicious software.
- **File Sharing:** Exchange of media over peer-to-peer networks (e.g. BitTorrent). Since these files come from untrusted sources, they pose a high risk of malware infections.
- **TLS/SSL Certificates:** TLS/SSL certificates are used to encrypt traffic over the Internet. Bitsight analyzes certificates and provides information about their effectiveness; e.g. whether they are signed using a secure algorithm.
- **TLS/SSL Configurations:** Whether a company's servers have correctly configured security protocol libraries, and support strong encryption standards when making encrypted connections to other machines.
- **Open Ports:** Which port numbers and services are exposed to the Internet. Certain ports must be open to support normal business functions; however, unnecessary open ports provide ways for attackers to access a company's network.
- **DNSSEC:** A protocol that uses public key encryption to authenticate DNS servers. BitSight verifies whether a company is using DNSSEC and if it is configured effectively.
- **Server Software:** The types and versions of server software that the organization exposes to the internet. Unsupported or outdated software often suffers from known, exploitable vulnerabilities.
- **Desktop Software:** Whether browser and operating system versions are kept up to date for laptops, servers, and other non-tablet, non-phone computers in a company's network which access the internet.
- **Mobile Software:** Similar to the above, except for mobile devices.
- **Patching Cadence:** How many systems within an organization's network are affected by critical vulnerabilities, and quickly the organization patches them (vulnerabilities are publicly disclosed holes or bugs in software that can be used by attackers to gain unauthorized access to systems and data).

- **Insecure Systems:** Devices within the organization's network observed to be unintentionally communicating with a third party (e.g. IoT devices reaching out to expired domains).
- **Web Application Headers:** This risk vector analyzes security-related fields in the header section of HTTP request and response messages. If configured correctly, these fields can help provide protection against malicious behavior, such as man-in-the-middle and cross-site scripting attacks.
- **Mobile Application Security:** If an organization publishes mobile applications on the Apple App Store or Google Play, Bitsight evaluates the security of those applications.
- **SPF records:** Properly configured SPF records help ensure that only authorized hosts can send email on behalf of a company by providing receiving mail servers the information they need to reject mail sent by unauthorized hosts. Bitsight verifies that a company has SPF records on all domains that are sending or have attempted to send email, and that they are configured in a way that helps prevent email spoofing.
- **DKIM records:** Properly configured DKIM records can help ensure that unauthorized parties can't send email that appears to originate from the organization's domains. Bitsight verifies that a company uses DKIM and has configured it in a way that prevents email spoofing.

Country	Indexes included
Australia	S&P/ASX 100 S&P/ASX 200 S&P/ASX 300
Canada	S&P/TSX Composite
France	CAC 40
Germany	DAX
Japan	Nikkei 225
United Kingdom	FTSE 100 FTSE 250
United States	S&P 500 Russell 3000

Company groupings
Based on board structures



69% Companies with only audit

26% Companies with specialized risk committees

5% Companies with neither

	Advanced security performance range 740 – 900	Intermediate security performance upper range 700 – 730	Intermediate security performance lower range 640 – 690	Basic security performance range 250 – 630	Average security performance	Median security performance	Total companies
Companies with specialized committees	45%	25%	20%	10%	710	720	1,062
Companies with only audit	41%	26%	22%	11%	710	710	2,839
Companies with neither	23%	15%	31%	31%	670	660	248

	Specialized risk committees	Companies with only audit committee	Companies without either committee	Total companies
Advanced security performance range 740 – 900	28%	68%	3%	1,710
Intermediate security performance range 640 – 730	25%	70%	6%	1,955
Basic security performance range 250 – 630	21%	63%	16%	484

Sector breakdown

Sectors	Number of companies
Financials	1,038
Industrials	634
Healthcare	590
Consumer Discretionary	479
Information Technology	430
Materials	306
Energy	205
Consumer Staples	191
Communication Services	165
Utilities	110

Sector breakdown of companies with advanced security ratings (GICS)

Sectors	Number of companies
Financials	559
Health Care	308
Industrials	174
Information Technology	162
Consumer Discretionary	151
Materials	123
Energy	95
Consumer Staples	59
Utilities	47
Communication Services	33

Sector breakdown of companies with basic security ratings (GICS)

Sectors	Number of companies
Industrials	118
Consumer Discretionary	85
Information Technology	60
Financials	51
Communication Services	51
Consumer Staples	35
Health Care	31
Materials	27
Energy	19
Utilities	6

S&P/ASX 300

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	260	90%	3	1.04%	700
Total number of companies with audit companies	275	95%	3	1.04%	700
Companies with audit committees without specialized committees	17	6%	0	0.00%	660
Companies with neither	10	3%	0	0.00%	750

FTSE 250

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Average cyber risk rating
Companies with specialized risk committees	119	48%	4	1.60%	700
Total number of companies with audit companies	250	100%	7	2.80%	710
Companies with audit committees without specialized committees	131	52%	3	1.20%	700

S&P/TSX Composite

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	101	45%	1	0.96%	700
Total number of companies with audit companies	217	96%	2	0.92%	710
Companies with audit committees without specialized committees	114	51%	0	0.00%	710
Companies with neither	9	4%	0	0.00%	700

FTSE 100

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	48	48%	4	4.00%	650
Total number of companies with Audit companies	100	100%	5	5.00%	650
Companies with Audit committees without specialized committees	52	52%	1	1.00%	650

S&P/ASX 100

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	93	98%	0	0.00%	690
Total number of companies with Audit companies	94	99%	0	0.00%	680
Companies with audit committees without specialized committees	3	3%	0	0.00%	620

DAX

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	5	13%	1	3.00%	620
Total number of companies with Audit companies	37	93%	2	5.00%	640
Companies with audit committees without specialized committees	31	78%	1	3.00%	640
Companies with neither	4	10%	0	0.00%	670

S&P 500

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	135	27%	19	4.00%	690
Total number of companies with Audit companies	500	100%	61	12.00%	680
Companies with Audit committees without specialized committees	365	73%	42	8.00%	670

Russell 3000

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	510	17%	56	11.00%	730
Total number of companies with Audit companies	2,975	98%	204	7.00%	720
Companies with audit committees without specialized committees	2,465	82%	148	5.00%	720
Companies with neither	8	0.3%	0	0.00%	720

S&P/ASX 200

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	182	93%	3	2.00%	690
Total number of companies with Audit companies	192	98%	3	2.00%	690
Companies with audit committees without specialized committees	10	5%	0	0.00%	620
Companies with neither	3	2%	0	0.00%	760

CaC 40

	Number of all companies	Percent of all companies	Number of tier 1	Percent of tier 1	Mean cyber risk rating
Companies with specialized risk committees	15	38%	2	5.00%	690
Total number of companies with Audit companies	39	100%	4	10.00%	660
Companies with Audit committees without specialized committees	24	62%	2	5.00%	650