Brown & Brown

PROPERTY & CASUALTY

Cyber and D&O Risk

The Dual Boardroom Threat

By, Caleb Blodgett and William Lester

Cyber risk has emerged as one of the most critical challenges for corporations, setting it apart from more traditional property and casualty risks. Unlike physical losses from fires or natural disasters, a cyber event can represent more than just a financial loss to a balance sheet. These events often expose vulnerabilities in a firm's governance and risk management capabilities, making them an essential test of leadership for directors and officers (D&Os).

For a public company, the stakes can be even higher: a significant cyber event can trigger dramatic share price declines as markets react to the disclosures and potential lawsuits from investors alleging shareholder loss or negligence in oversight or preparedness. Understanding the relationship between cyber and D&O risk and exploring the impact of alleged shareholder loss following cyber events is essential.

Understanding the Cyber and D&O Connection

Cyber: A Top Concern for Directors and Officers

Cyber risk consistently ranks among the top concerns for directors and officers[1], reflecting its role in corporate stability and the level of influence D&Os have over managing this risk. While awareness is growing, many firms remain unaware of the link between cyber incidents and D&O liability. This disconnect can leave firms ill-prepared for financial and operational fallout following a cyberattack.

SEC Cyber Disclosure Rules: A New Era of Accountability

Regulatory requirements have evolved to reflect the heightened importance of a board's role in cyber risk management. The SEC's updated 8-K disclosure rules mandate that companies disclose material cybersecurity incidents within four business days of determining their impact, including qualitative and quantitative assessments. Yet, compliance has been inconsistent: 73% of early disclosures from firms did not determine materiality, suggesting firms struggle to quantify the full extent of costs[2]. This gap in preparedness may leave D&Os vulnerable to claims of insufficient governance and oversight.

1. Allianz Risk Barometer 2024: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

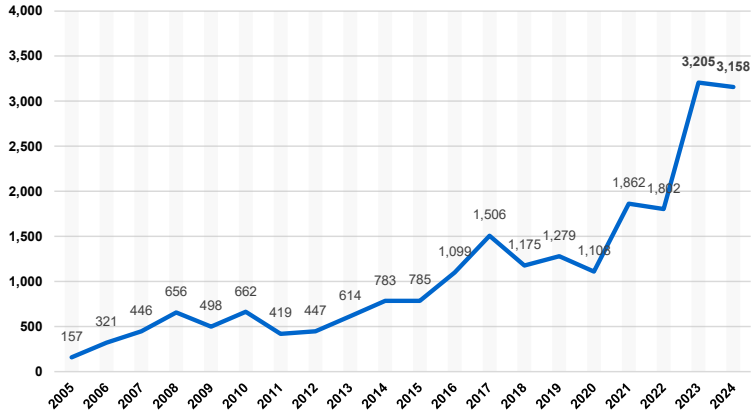
2. https://www.debevoise.com/insights/publications/2024/03/100-days-of-cybersecurity-incident-reporting

The Rising Frequency of Cyber Events

The frequency and cost of breaches continue to rise at an alarming rate[3]. While not always publicly reported, ransomware attacks and business interruption compound this risk, with numerous studies and high-profile events showing their prevalence and damage[4]. This rising threat highlights the importance of strong cybersecurity preparedness to avoid these incidents escalating into a crisis with board-level implications.

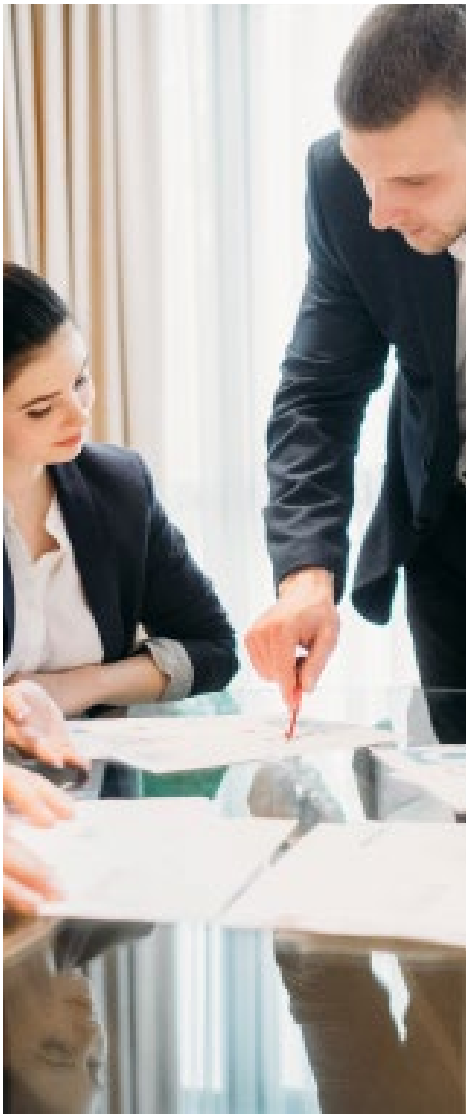
ANNUAL NUMBER OF DATA COMPROMISES IN THE UNITED STATES

2005 to 2024



The Subsequent D&O Liability

As cyberattacks rise, so have D&O claims tied to these events. Securities class action (SCA) filings related to data breaches have surged in recent years[5], driven by investors alleging economic losses often tied to drops in share price following the disclosure of a cyber event. While public companies are particularly vulnerable to these securities suits, privately held firms are not immune[6].



The financial stakes of these claims can be substantial. In 2024 alone, just three data breach-related SCAs resulted in settlements totaling $560 million,[5] marking some of the largest payouts in history. Even when these suits are unsuccessful, the equity declines that often follow cyber events remain highly relevant to corporate leadership and investors. Shareholder value can be eroded by short-term market reactions and long-term underperformance, making cyber risk a persistent concern for investors and boards alike.

Shareholder Loss Following Cyber Events

Cyber incidents often result in sharp, immediate declines in stock prices as investors react to the potential operational and reputational fallout. Some studies have reported average stock price drops of over 7%[5] immediately following a breach disclosure. However, share declines can be far more extreme for certain industries and high-profile events.

Prolonged underperformance of the share price is another critical consequence of cyber events. It can take an average of 46 days to rebound to pre-breach levels.[5] Even after recovery, firms can still underperform market indices long-term. Research conducted by Moody's finds that even moderate-impact cyber events can result in abnormal equity returns over a longer time period, with average cumulative underperformance over a 12-month period of over 5%.[7]

3. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

4. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

5. https://corpgov.law.harvard.edu/2024/08/21/data-breach-securities-class-actions-record-settlements-and-investor-claims-on-the-rise/#11

6. https://www.dandodiary.com/2017/09/articles/securities-litigation/though-private-company-uber-hit-securities-class-action-lawsuit/

7. https://www.bitsight.com/resources/moodys-analytics-impact-cyber-security-management-practices-likelihood-cyber-events-and

Securities Class Action Suits: Alleged Shareholder Loss

To understand the magnitude of shareholder loss for more extreme breaches, consider the share price drops referenced in securities class action filings related to cyber events.

Zywave's Loss Insight Feed for cyber and D&O risk is used to identify a set of SCA lawsuits tied to cyber events. For this analysis, all references to stock price declines are extracted from the corresponding complaint filings and reviewed. Many of these complaints cite publicly available news sources—rather than conducting detailed market analyses—to establish the basis for shareholder loss surrounding the class period. Occasionally, a complaint will outline multiple stock price drops over multiple trading days. In these cases, the cumulative return over all referenced trading days is calculated.

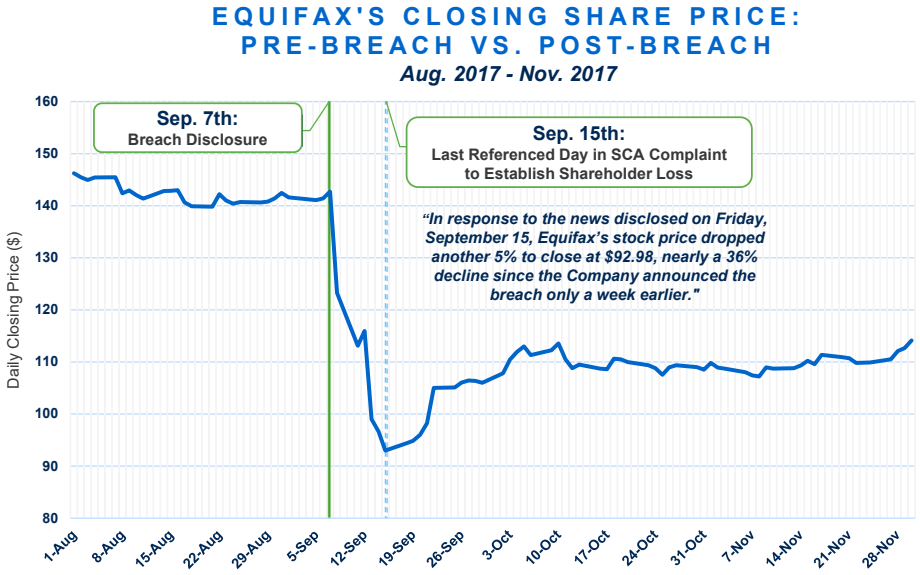


Figure 2: Equifax Closing Share Price: Aug. 2017 – Nov. 2017[8]

The full distribution of share declines is shown below:

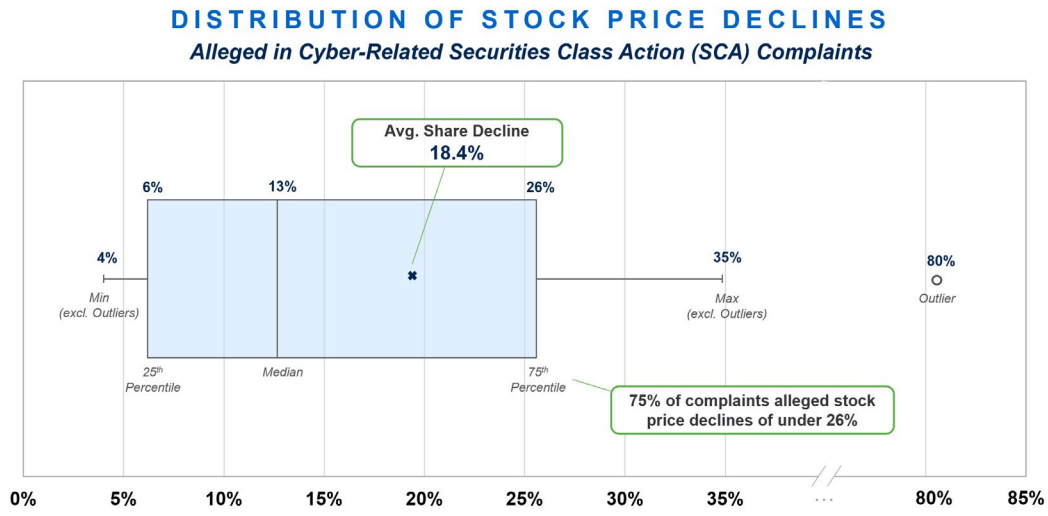


Figure 3: Securities Class Action Complaints Following Cyber Events – Alleged Shareholder Losses

The alleged losses are significant, with the average share drop for the sample of cyber-related SCA filings being over 18%. While complaints tended to focus on the immediate market reactions following the disclosure of an event, rather than any long-term underperformance, the distribution provides important context for firms looking to understand potential D&O losses following a cyber event.

8. S&P Global's Compustat® Financials: https://www.marketplace.spglobal.com/en/datasets/compustat-financials-

However, cyber-specific data remains limited, with few finalized SCA settlements from which to draw. To address this gap, consider the broader population of all SCA suits to understand how market capitalization declines can correlate with potential settlements. Below, the declines in market capitalization are in dollars rather than percentages, since larger, well-capitalized firms will generally have larger market cap declines and deeper pockets for potential payouts . This broader dataset of events allows us to approximate potential D&O losses from cyber events, even when direct cyber-related SCA precedent is scarce.

MARKET CAPITALIZATION DECLINE[9] VS. SECURITIES CLASS ACTION (SCA) SETTLEMENT[10]

Source: Advisen Public D&O Loss Database

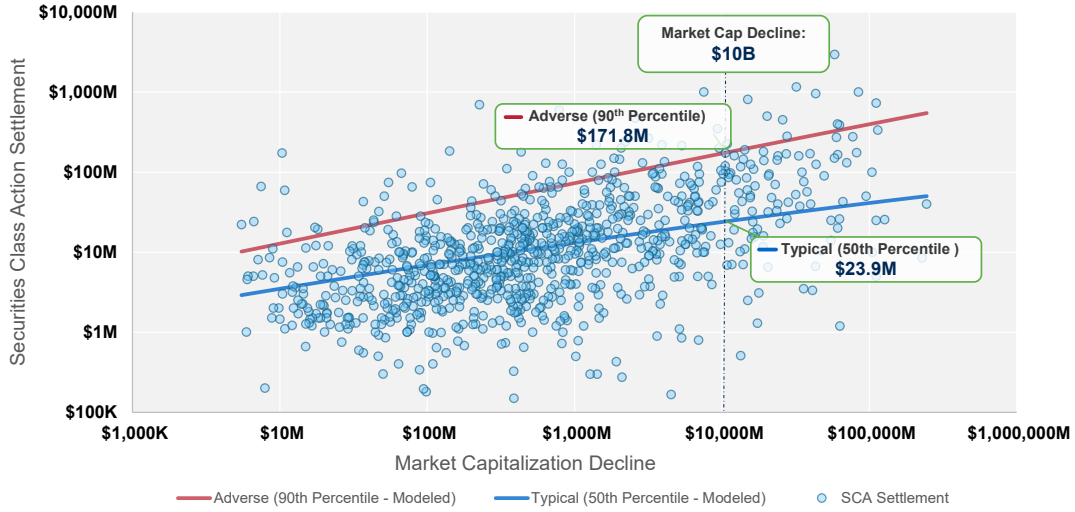


Figure 4: SCA Settlement Amount vs. Five-Year Peak Floating Market Capitalization Decline

The fitted distributions above show a clear correlation between market capitalization declines[9] and securities class action[10] settlements. This relationship, however, reinforces the many sources of financial risk that public companies face following a cyberattack. Firms first encounter uncertainty in the direct costs of a cyberattack, from extortion demands to liability and incident response costs. Following an attack, they face uncertainty in the magnitude of market cap declines, as indicated in the distribution of stock price declines observed in cyber-related SCA filings. Finally, even with a given market cap decline, D&O liability can vary significantly.

Understanding these different dimensions of risk is important for refining cyber risk management and insurance strategies. Modeling various distress scenarios and their financial impacts, including potential market cap declines and corresponding SCA settlements, can enable more informed decisions regarding insurance coverage, financial reserves and governance measures. Such proactive modeling and the recommendations provided in the next section will help companies better prepare for the financial implications of cyber incidents and mitigate potential shareholder losses and D&O claims.

9. Market capitalization decline for an SCA suit is measured by comparing the company's five-year historical peak floating market capitalization to its floating market capitalization at the beginning of the securities suit filing year.

10. Filing years span 2005 to 2022; certain SCA suits have been excluded due to their limited applicability to the broader market of firms.

Managing the Dual Threat: Recommendations for Firms

Effectively managing the interconnected risks of cyber and D&O requires a proactive approach.

1 Understand Existing Cyber and D&O Programs

- Regularly review policies to help ensure no critical risks are excluded
- Engage a broker skilled in both cyber and D&O insurance to design complementary policies for coverage and pricing efficiencies

2 Integrate Quantitative Assessments into Risk Management

- Quantitative modeling plays a key role in understanding the potential financial impacts of D&O and cyber events and ensuring compliance with regulatory requirements
- Consider using integrated D&O and cyber modeling to set appropriate limits and coverage that aligns with risk appetite
- Quantify the risk-reward tradeoffs to understand the costs and benefits of increasing or reducing coverage and using alternative risk financing strategies

3 Prioritize Preparedness and Stakeholder Communication

- Recognize the main risk factors and risk mitigation approaches available to your firm, from key cybersecurity controls to incident response solutions
- Proactively communicate risk management strategies to build trust and resilience with investors and board members
- Routinely evaluate loss exposure, governance structures and cybersecurity controls to help ensure alignment with the evolving legal landscape and emerging cyber risks

How We Can Help

At Brown & Brown, our specialization in cyber and D&O risks can help your organization assess its exposure, strengthen governance practices and help ensure compliance with emerging requirements. Contact us today to discuss how we can support your board in understanding coverage, mitigating risks and safeguarding shareholder value.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com