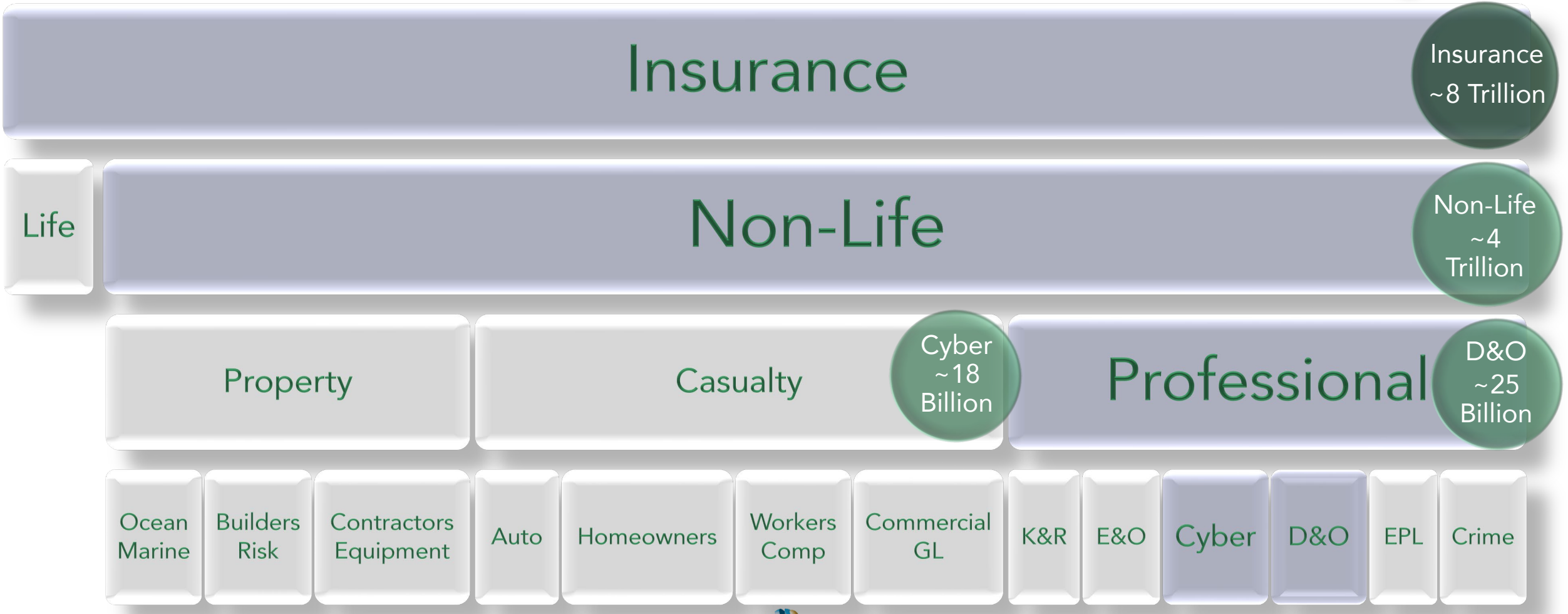
The Intersection of D&O and Cyber Insurance: Navigating Coverage, Exclusions, and Claims

April 22, 2025

Where Does Cyber/D&O Fit?



Coverage – D&O vs. Cyber

Directors & Officers

Coverage "A"

Personal asset protection for D&O's

- Non-Indemnifiable Claims
- Bankruptcy
- Corporation refusal to pay

Coverage "B"

Corporate Asset Protection

- Reimburses corporation for covered indemnifiable claims

Coverage "C"

Corporate Asset Protection

- Covers liability of corporation in covered securities claims

Cyber

First-Party

- Notification Costs
- Legal Fees
- Forensics
- Contingent/Business Interruption

- PR
- Extortion
- Data Recovery/Replacement

Third-Party

- Customer Suits
- Third-party suits (Tech E&O/MPL)
- PCI–DSS fines

- Privacy Regulatory
- Media liability
- Reputation

Claim Triggers

Directors & Officers

- Breach of fiduciary duty
- Misrepresentation in financial statements
- Regulatory investigations (SEC, DOJ, FTC)
- Shareholder lawsuits and derivative claim
- M&A litigation and bankruptcy-related claims

Cyber

- Ransomware and extortion
- Data breaches and privacy violations
- Business interruption and system failures
- Third-party liability and regulatory fines

- Professional Services
- BI/PD
- Prior Acts/Knowledge
- Conduct Exclusion
- Contractual Liability

Exclusions

- Bodily Injury/Personal Misconduct
- D&O Exclusion ('33/'34 Act)
- Insured vs. Insured
- Prior Acts/Knowledge
- Gained Advantage/Prior Knowledge

Coverage Scenarios

Scenario	D&O	Cyber
Director is sued for negligence	Yes	No
Data breach exposes customer data	No	Yes
Company faces regulatory investigations over a breach	Possibly (if it's about governance)	Yes (for the breach itself)
Ransomware attack halts operations	No	Yes
Mismanagement of cybersecurity policies leads to investor lawsuits	Yes	Possibly (D&O management liability; Cyber for incident costs)

Priority Scenarios

Business Type	Priority	Why
Tech or SaaS Company	Cyber > D&O	High exposure to data risk, breaches, and customer data. D&O is still valuable for investor protection.
Financial Services / Fintech	Both are critical	Highly regulated, data-rich, with investor pressure. Both data liability and governance risk are high.
Healthcare / Medical Practices	Cyber > D&O	HIPAA and patient data make Cyber essential. D&O is still helpful for corporate governance issues.
Startups with Investors or a board	D&O > Cyber	Early-stage companies are more exposed to founder/board-related legal actions. Cyber grows in importance as the company grows.
E-commerce / Retail	Cyber > D&O	Large amounts of customer data and online transactions = more cyber risk. D&O is helpful for public-facing companies.
Public Companies	D&O > Cyber	Board and leadership liability is higher. Cyber is still important if customer data is stored.

Litigation Trends

Increase in Class Action Lawsuits Post-Breach	• Failure to protect PI (Personally Identifiable Information) • Negligence or breach of contract • Violation of data privacy laws (e.g., CCPA, BIPA, GDPR)
Regulatory Enforcement is Increasing	• FTC, SEC, state attorneys general, and international regulators are more aggressive in pursuing fines and penalties
Securities Litigation Tied to Cybersecurity	• Shareholders suing companies for failing to disclose cyber risks or breaches in a timely or transparent manner
Litigation Around Ransomware Incidents	• Companies that pay ransoms (or refuse to) may face legal action from customers, partners, shareholders
Claims	• Rising claims cost from a defense perspective that is mirroring class actions and derivative claims in D&O

Cybersecurity, a Perennial D&O Risk Issue, Remains Relevant

February 2024

Alphabet settles Google+ data breach securities class action lawsuit for $350 million.

- Largest ever cybersecurity-related securities suit settlement?
- Underscores the fact that cybersecurity remains a significant source of corporate and securities litigation exposure.

Continuing SEC Cybersecurity Enforcement

Trusted SAFETY NATIONAL Since 1942

July 2024

R.R. Donnelly: Settled enforcement action following cyber incident at the company

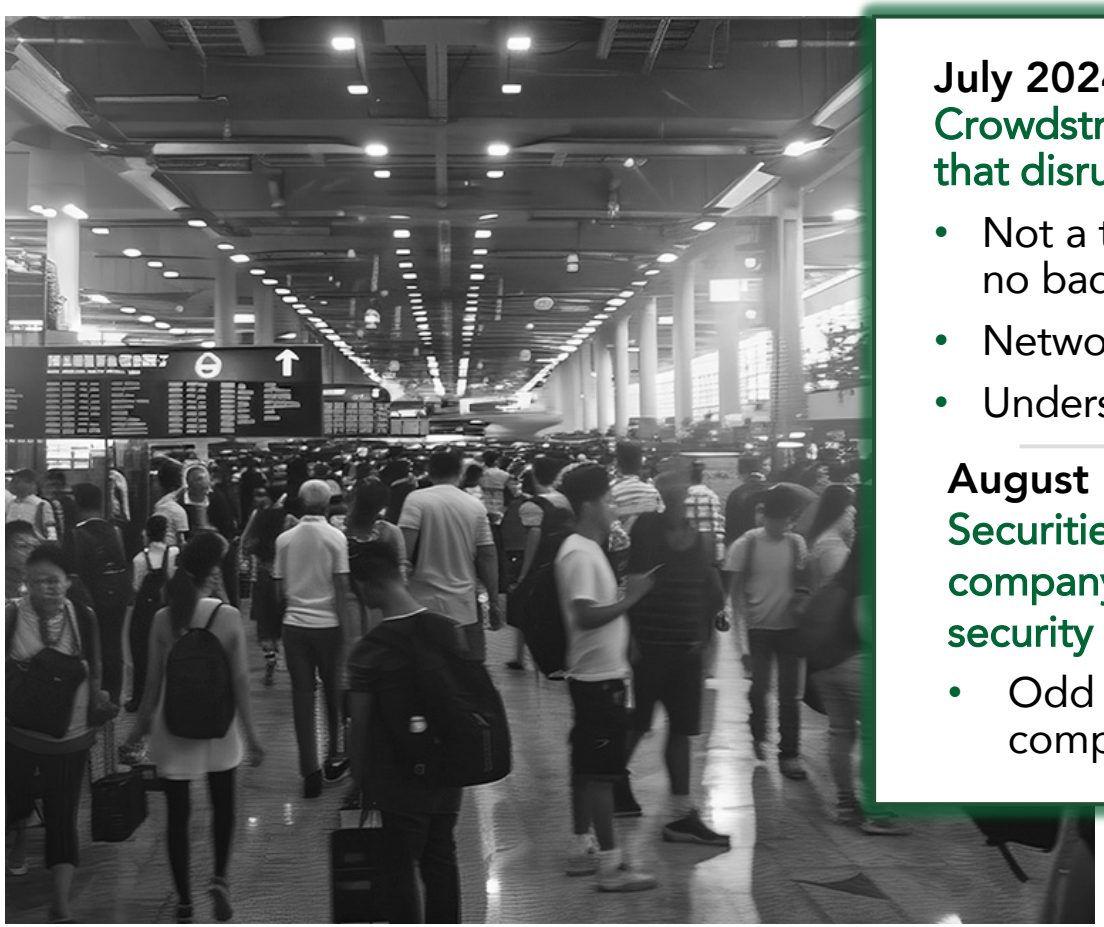
- SEC alleged the company's accounting and disclosure controls were deficient.

October 2024

SEC announces settled enforcement actions against four companies affected by SolarWinds data breach.

- SEC alleged misleading disclosures regarding the cyber incidents.
- One of the four is also alleged to have deficient accounting and disclosure controls.

Cybersecurity-Related D&O Suits Continue to Be Filed – Allegations Have Changed



July 2024:

Crowdstrike hit with securities suit following massive IT-systems outage that disrupted U.S air service

- Not a typical cybersecurity suit: No data breach, no data disclosures, no bad actor
- Network systems security suit rather than cybersecurity
- Underscores the importance of systems integrity and stability

August 2024:

Securities suit filed against PDD Holdings after revelations that the company itself placed malware on its customers' devices (overrode security controls and allowed PDD to access user information)

- Odd variant; no third-party actor involved, the hostile actor in the company itself

SEC Cyber Disclosure Guidelines

Trusted SAFETY NATIONAL Since 1942

Effective December 2023
Requires periodic disclosure regarding cyber governance and controls, as well as incident-specific disclosure of data breaches.

Recent study shows that between December 2023 and October 2024, 48 companies made 75 cyber incident disclosures (60%) increase.

Recent commentary suggests SEC under Paul Atkins may withdraw or non-enforce the guidelines or various parts.

Republican Commissioner dissents in cyber enforcement actions suggest the agency will change their policy on bringing charges based on alleged accounting and disclosure deficiencies.

Key Takeaways

Different Focus, Different Protection

Cyber Liability: Protects the organization from cyber risks (e.g., data breaches, ransomware).

D&O Insurance: Protects executives personally from lawsuits related to mismanagement or leadership decisions.

D&O/Cyber Can Work Together

Cyber covers technical response and damages.

D&O may respond if executives are blamed for negligence in preventing cyber risks.

Business Type Determines Priority

Tech and data-heavy businesses prioritize Cyber.

Investor-backed and regulated businesses need D&O (often both).

Coverage Gaps Without Both

Cyber doesn't protect personal liability.

D&O doesn't pay for breach response, IT forensics, or ransomware.

Claims-Made Policies Require Timely Reporting

Both are usually claims-made; ensure claims are reported properly and retroactive coverage is in place.

THANK YOU