

Maximizing Insurance Coverage for Today's Changing Risks: D&O, Cyber & Privacy Coverage

John Wilson, Colleen Smith & Drew Gardiner

LATHAM & WATKINS^{LLP}

D&O Insurance

D&O Insurance Coverages

Standard D&O Policy combines three coverages under single limit:

- Side A: Pays non-indemnified loss of individual officers and directors
 - Not subject to any retention / deductible
 - Triggered whenever Company cannot indemnify. Two most common scenarios are: 1) company insolvency and 2) derivative settlements
- Side B: Balance sheet protection – reimburses Company for amounts it pays in indemnification of officers and directors
- Side C: Coverage for securities claims against public companies (including derivative claims and certain shareholder demands); broader coverage for claims against private companies

Excess Side A / DIC (Difference in Conditions) Policies

- Typically written to attach upon exhaustion of underlying A/B/C policies, but can be written on stand-alone basis if Company chooses to forgo balance sheet protection and self-insure for Side B/C losses
- **DIC enhancement requires Insurer to drop down and provide coverage if underlying coverage is unavailable for any reason:**
 - Insolvency of underlying insurer
 - Denial of coverage by underlying insurer
 - Application of automatic stay in bankruptcy precluding coverage under A/B/C policies, which are deemed property of estate
- **Independent directors can also obtain IDL (Independent Directors Liability) Policy -- Side A policy with limits reserved solely for them**

Private vs Public Company D&O Insurance

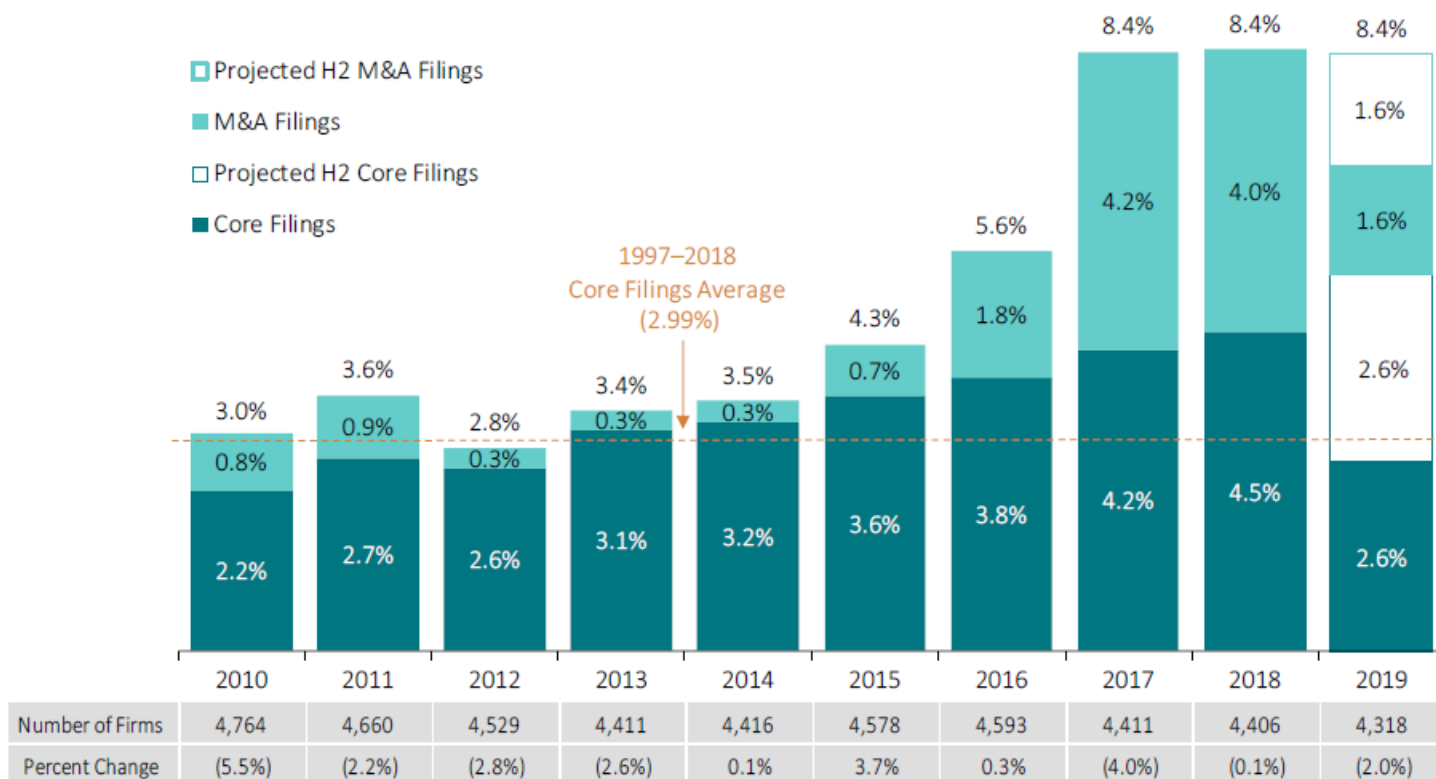
- **Private company premiums are less expensive due to minimal securities litigation risk**
- **Side C coverage can cover a variety of different claims against a private company, not just securities claims**
 - Important to review for potential coverage for any claims asserted
- **Need to carefully scrutinize any “major shareholder” exclusion and “insured vs insured” exclusion, each of which can bar coverage for many claims Company may expect to be covered**

D&O Market Conditions

- **According to reports, the D&O market is entering its fifth or sixth year of unprofitability.**
 - **Increased class action filings in last several years**
 - **Increased frequency of companion derivative lawsuits**
 - **Increased costs associated with early / electronic discovery**

Frequency of Securities Class Actions

- **Securities class actions are increasing in frequency.** Securities class action core filings are projected to affect up to 5.2% of U.S. public companies in 2019.



Source: Cornerstone Research, *Securities Class Action Filings: 2019 Midyear Assessment at 15* (2019).

Increase in IPO Related / '33 Act Class Actions

- **The U.S. Supreme Court's decision in *Cyan Inc. v. Beaver County Employees Retirement Fund* has resulted in a sharp uptick in Securities Act cases.**
 - After *Cyan*, plaintiffs may bring, and keep, these claims in state courts, which often allow early discovery and are less likely than federal courts to dismiss securities claims.
 - Section 11 class actions increased 52% in 2018 over 2017, driven primarily by increased filings in state court. A further increase is projected for 2019.
 - Between 2010 and 2018, IPO-related securities litigation followed approximately 25% to 30% of IPOs.

Sources: Cornerstone Research, *Securities Class Action Filings: 2019 Midyear Assessment* at 13 (2019); Cornerstone Research, *Securities Class Action Filings: 2018 Year in Review* at 24, 25 (2019); ISS Securities Class Action Services, *The Uncertain Role of IPOs in Future Class Actions* (2018).

The Impact of *Cyan*

1933 Act Class Action Filings	Annual Average 2010-2017	2017	2018	1H2019
State Courts Only	4	2	15	12
Federal Courts Only	16	11	11	6
Parallel Filings in State and Federal Courts	6	14	16	7
Totals	26	27	42	25

Sources: Cornerstone Research, *Securities Class Action Filings: 2019 Midyear Assessment* at 14 (2019); Woodruff-Sawyer & Co., July 25, 2019.

D&O Market's Response

D&O Insurers have responded by:

1. Decreasing capacity
2. Increasing premiums
3. Narrowing coverage terms

Decreasing Capacity

- D&O capacity declined in 2019 for the first time in over a decade
- Some major insurers have exited private company market entirely
 - AIG has curtailed aggregate limits by \$20 billion, and reduced primary limits by over 40% in 2019
- The limit each insurer is willing to write for any given risk—even in excess layers—continues to shrink
 - The most any one insurer will issue is \$10M (down from \$15M), and only \$2.5M for most IPOs

Increasing Premiums & Retentions

- Most companies are now experiencing increases in D&O policy premiums, even without any claims experience
- D&O insurers are seeking to achieve aggregate rate increases of at least 25% for major public accounts
- Small private accounts are typically seeing at least 10% premium increases
- Underwriters are simultaneously increasing retentions, in some cases very significantly
 - Most IPO policies carry at least \$20M retention

Narrowing Coverage Terms

- Insurers actively seeking to undo improvements in policy language that have been incorporated in recent years
 - Recent blog post advises insurers on coverage enhancements they should seek to reverse, and additional exclusions to add
 - Particularly troubling is a suggestion to “revisit severability for conduct exclusions”
 - Severability provision prevents insurers from denying coverage for one innocent individual based on wrongful conduct of another insured
- **Very** important to review terms at renewal to ensure—at a minimum—that insurers are not limiting coverage

Potential Solutions to Pricing Challenges

- **Increasing proportion of Side A vs A/B/C coverage should be evaluated:**
 - Less expensive, but zero balance sheet protection
 - Still effective way to protect personal assets of officers and directors
- **Consider use of retrospective premiums and co-insurance:**
 - Allows Company to retain portion of the risk – putting skin in the game – when markets are not accurately assessing risk of future claims
- **Insurers are not shy about admitting they are trying to recoup losses from prior years**
 - Yet premiums for future years should be based on actual risk

Other Pitfalls to Navigate

Whenever changes are made to D&O program structure, potential complications arise:

- Insurers of new policy may seek to include “prior acts” exclusion barring coverage for claims based on conduct occurring prior to policy period:
 - Language should be carefully scrutinized and narrowed or eliminated
 - If exclusion cannot be removed, may need to negotiate “tail coverage” for expiring policy period to cover future claims based upon past conduct
- New policies can also exclude coverage for claims related to claims previously reported to a prior insurer
- **Insurers seek to greatly restrict policyholder’s selection of counsel to minimize financial outlay in the event of a covered loss**
 - Often flies in face of insureds’ expectations

Bankruptcy Considerations

Side A Coverage is particularly important – provides coverage in the event the company cannot indemnify

- A/B/C policies are property of the estate and subject to an automatic stay in bankruptcy court; but Side A policies are not
- Courts reach different conclusions on whether proceeds of A/B/C policies are property of the estate
- Insurers typically require a “comfort order” authorizing payments to individuals notwithstanding automatic stay

“Priority of Payments” confirm that in the event of competing demands for coverage, payment of non-indemnified loss of individuals should be prioritized

LATHAM & WATKINS^{LLP}

Cyber & Privacy Insurance

Cyber Attacks Grow in Prevalence and Sophistication



Gangs Beyond Borders

California and the Fight Against Transnational Organized Crime

March 2014

Kamala D. Harris
California Attorney General



Chapter Five

High-Tech Crime: A New Frontier for Transnational Criminal Organizations

The emergence of the Internet and of a global society linked together by high-speed information networks has transformed the ways in which businesses, governments, and individuals communicate and engage in commerce. Sellers on one side of the world can now advertise directly to buyers on another side of the world. Sales and financial transactions can take place instantaneously and anywhere there is an Internet connection. And goods and services themselves are increasingly being delivered digitally through the Internet. The benefits of these transformations for the global economy, and ultimately for consumers, have been dramatic. At the same time, these transformations have also given rise to a new set of dangers, as some of the same technologies that enable people across the globe to connect instantaneously with one another and exchange money or information also facilitate criminal exploitation:

No Silver Bullet

- Any useful computer system can be made to do malicious things
 - No technology can identify malware with 100% accuracy
 - As long as there are flaws in software or the people who use it are not perfect, there will be successful cyber attacks
- Today's cyber attackers do not need to be computer experts. The know-how, tools, and services needed are all for sale on the "Dark Market."



Data Breach Incidents

Date Made Public	Incident
November 2018	Marriott International Marriott announced that between 2014-2016, it had been hacked by a Chinese intelligence group, suffering the largest known breach of personal data believed to be conducted by a nation-state. The breached information included contact information, passport numbers, travel information and credit card data for approximately 100 million customers.
July 29, 2017	Equifax Attacked through an application vulnerability on its website, Equifax suffered a breach of the Social Security numbers, birth dates, addresses, and drivers license information for nearly 150 million consumers.
September 2016	Yahoo! Between 2013-2014, Yahoo! was victimized by what are considered by many to be the largest data breaches in history. The attacks collectively compromised the real names, email addresses, birth dates, telephone numbers, passwords and security questions/answers of 3 billion user accounts. The impact of the breaches was estimated to exceed \$350 million.
January 29, 2015	Anthem, Inc. The information stolen from the insurance giant includes names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data. Anthem said there is no evidence that credit card or medical information was compromised. While damage is still being assessed, the compromised database contained up to 80 million customer records.
December 13, 2013	Target Corp. Attackers leveraged access to a third party network of Target's, where they were able to penetrate and move about undetected on Target's network and upload malware programs on the company's Point of Sale system. More than 110 million people were affected, and cost of the breach was estimated to exceed \$160 million.

Cyber Insurance

Coverage Areas Can Include:

1. Data Loss
2. Business Interruption
3. Privacy Liability
4. Notification and Compliance Expenses
5. Crisis Management – Forensic Investigations and Public Relations
6. Reputational Harm
7. Content Liability
8. Regulatory Investigations

Cyber Insurance Coverages

Case Type	Insuring Agreements
Digital Data Breach, Loss, or Theft	Crisis Response and Notification Expenses
	Electronic Theft
Identity Theft/Fraudulent Use or Access	Privacy Injury Liability
Phishing, Skimming	Privacy Event Response
Improper Disposal/Distribution, Loss or Theft (Printed Records)	Crisis Response and Notification Expenses
Digital Asset Loss or Theft	Privacy Injury Liability
	Loss or Damage to Insured's Systems
	Electronic Theft
Cyber Extortion	Threats or Extortion Response
System/Network Security Violation or Disruption	Cyber Liability/System Security Liability
	Crisis Response and Notification Expenses
	Business Interruption And Extra Expense
	Loss or Damage to Insured's Systems
Improper Collection of Digital Data	Cyber Liability/System Security Liability
	Crisis Response and Notification Expenses
	Electronic Theft
Privacy Violations	Privacy Injury Liability
	Privacy Event Response

Basic Data Security and Privacy Liability Coverages

Network Security Liability

- Claim expenses and damages emanating from network and nonnetwork security breaches
 - Denial of service attack
 - Transmission of a virus
 - Theft of data

Privacy Liability

- Claim expenses and damages emanating from violation of a privacy tort, law, or regulation
- Claim expenses and damages emanating from a violation of a law or regulation arising out of a security breach

Extortion Payments

- Reasonable and necessary expenses and any funds or property paid (varies by company)

Privacy Event Expense Reimbursement

- Expense reimbursement for third-party forensics costs
- Public relations and Legal
- Mandatory notification costs (comply with security breach notification laws)
- Voluntary notification costs
- Credit monitoring
- Call center
- ID Theft Insurance

Privacy Regulatory Proceedings and Fines

- Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding
- Damages/fines (varies by market) Consumer Redress Fund
- Privacy regulations fines
- PCI DSS fines and assessments(varies by market)

Third Party Coverage

- Damages Claims
 - from violation of a privacy tort, law, or regulation
 - from a violation of a law or regulation arising out of a security breach
- Defense Costs
 - third party claims and regulatory defense
- Media Liability
- Data Loss
- Intellectual Property Losses



First Party Coverage

- Remediation Costs
- Fines/Penalties
- Business Interruption
- Damage to Systems
- Intellectual Property
- Computer Fraud
- Funds Transfer
- Extortion



Remediation costs to respond to the breach

- Investigation/forensics to determine cause and extent of breach
- Public relations
- Customer notification
- Credit monitoring for customers
- Identity theft resolution services
- Call centers
- Costs to re-secure, re-create, and/or restore data
- Legal services/advice
- “Crisis management” services

Exclusions

- Contractual Liability
- Criminal Conduct
- Unfair Business Practices
- Content Theft
- Unauthorized Collection of Customer Data
- Intentional or Fraudulent Acts
- Terrorism, Hostilities, and claims arising from “acts of foreign enemies.”



Cyber Insurance Marketplace



Cyber Policies developed as

Reimbursement policies that allowed the insured to hire vendors but many companies did/do not have an effective cross-border data breach contingency plan.



New Development – Expert Vendor Panels

Established breach panels – particularly legal, forensics, and credit protection services.

Cross- border and multiple language capability for call center support.

Data breach coach.



Other Considerations

Definition of Confidential Information

Aggregate and other limits

Retroactivity

Time Limitations

- business interruption
- credit monitoring and other breach response

Steps in Purchasing Cyber Risk Insurance

- Key Market Invitations
- NDA signed by all invited insurers
- Project Plan with Mutual Milestones + Key Dates
- Data breach response coordination with client's crisis management plan and preferred vendors
- Short Form Application
- Policy Design Document w/Detailed Specifications
- Assistance with PP Briefing document and Presenter Rehearsal
- Underwriting briefing (one for all markets)
- Debrief with client and negotiations
- Finalize program and bind
- Timely issuance of master and local policies (if needed)



LATHAM & WATKINS^{LLP}

Questions?

Meet Your Speakers



Drew T. Gardiner

San Diego
email: drew.gardiner@lw.com
Phone: +1.858.523.5472

Drew Gardiner counsels clients on strategies for maximizing insurance coverage and represents policyholders in complex insurance coverage and bad faith disputes. Mr. Gardiner has prosecuted coverage claims involving a variety of first- and third-party policies, including commercial general liability, directors and officers (D&O) liability, errors and omissions and environmental impairment policies.



John M. Wilson

San Diego
email: john.wilson@lw.com
Phone: +1.858.523.5463

John Wilson's practice focuses on representing policyholders in complex insurance coverage and bad faith disputes, as well as environmental and business litigation. Mr. Wilson represents clients at all stages of litigation, from motion practice to trial and through the appellate process, in federal and state court litigation, international arbitration, and high stakes mediation.



Colleen C. Smith

San Diego
email: colleen.smith@lw.com
Phone: +1.858.523.3985

Colleen Smith, an experienced trial lawyer and Local Chair of the San Diego Litigation & Trial Department, represents emerging and Fortune 500 companies and their officers and directors in high-stakes complex litigation. Ms. Smith has secured major trial victories for clients facing enterprise-threatening liability, including in the first securities class action to go to trial in over a decade. In that matter, the jury reached a unanimous verdict in the client's favor on the majority of claims, awarding miniscule damages. Ms. Smith regularly defends companies and their executives against private plaintiffs claiming disclosure fraud, often achieving early dismissals on motion practice.

Disclaimer

Although this presentation may provide information concerning potential legal issues, it is not a substitute for legal advice from qualified counsel. Any opinions or conclusions provided in this presentation shall not be ascribed to Latham & Watkins or any clients of the firm.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.

© Copyright 2020 Latham & Watkins. All Rights Reserved.