NEWFRONT | ACC Association of Corporate Counsel SAN FRANCISCO BAY AREA

LIFE SCIENCES

Insuring Life Sciences Update 2025: Cyber Considerations for Legal Leaders

March 6, 2025

Speakers

Jennifer Wilson
Head of Cyber

Newfront

Dan Lindell
SVP, Executive Risk Solutions Practice

Newfront

Brandon Settle
AVP, Life Science Practice

Newfront

Caryn McDowell
Director

California Life Sciences

Agenda

01
Cyber Risk for Life Sciences

02
Management Liability Insurance

03
Top 10 Best Practice Insurance Management Processes

01

Cyber Risk for Life Sciences

Cyber is No Longer just About the Data

SUPPLY CHAIN – CROWDSTRIKE

Situation: A coding error in a Crowdstrike file caused a widespread system crash of a Windows driver which resulted in the blue screen of death (BSOD) error pages.

Impact: This caused massive global business disruptions. Estimated costs of **$5B**. Raising concern about risks and vulnerabilities of our interconnected digital infrastructure.

CHANGE HEALTHCARE RANSOMWARE ATTACK, 2024

Situation: Ransomware attack that affected ability to process prescription payments.

Impact: Over forty class action lawsuits as of February 2025, and estimated $2.9B in costs to date.

Cyber coverage matters: A security failure in a single business network can lead to widespread impact, including loss of revenue, reputational harm, and extra expenses.

Newfront POV

HONG KONG DEEPFAKES, 2024

Situation: Hacker tricked employee into thinking he was speaking with CFO via video and voice manipulation.

Impact: Loss of **$25M+**

Why Cyber coverage matters: Insurers are now more likely to implement the “call-back” requirement, MFA, and end-to-end encryption.

Newfront POV

Cyber Attacks by the Numbers

There are only two types of companies: Those that have been hacked, and those that don't know they've been hacked.

-Robert Mueller,
Former FBI Director

$5M

Average cost of a data breach attack for life science sector

53%

of digital medical devices in the U.S. are at risk of cyber attacks

$2.9B

Estimated costs resulting from Change Healthcare ransomware attack

$75M

Ransom amount paid by Cencora, Inc as a result of data breach attack in 2024.

6M

Number of individuals impacted by PharMerica Data Breach of 2023

$1.3B

Cost to Ascension Health following ransomware attack in May 2024. System outage impacted patient care, testing, and medication treatment

Why Cyber Risk Insurance for Life Science?

1. **Data Breaches –** Life science companies collect and store large volumes of sensitive data. A data breach could result in third party litigation, business interruption & extra expense costs, and reputational damage as well as regulatory fines.

2. **Ransomware & Business Interruption –** Ransomware remains the leading type of cyber attack, year over year. A ransomware attack could halt research, disrupt clinical trials, or shut down manufacturing supplies for medical devices. The average downtime following a ransomware attack is 23-59 days.

3. **Regulatory & Compliance –** Life sciences are highly regulated industries, with strict guidelines from the FDA, HIPAA, GDPR, and other regulatory bodies. A cyber incident could lead to mandatory reporting requirements, audits, and fines.

6. **Wrongful Collection** – Third party liability related to wrongful collection of data, including pixel tracking, and biometrics have steadily increased in frequency and severity over the past 4 years. These could be a result of improper consent and unlawful sharing of data.

7. **Social Engineering** - Cybercriminals use manipulation and impersonation tactics to deceive individuals into sharing sensitive information, transferring funds or credentials. High value IP makes life science a prime target for cybercrime.

8. **Supply Chain –** A cyber event on a dependent vendor can result in significant business interruption and extra expense. This can be related to a malicious attack or non-malicious outage. (Change Healthcare, Crowdstrike)

Thinking About Limit Adequacy

Considerations when determining limit adequacy / program structure

Risk Tolerance

- What is the Company's approach to Insurance?
- Retention vs. Premium?

Business Interruption

- Average downtime following a ransomware attack is 25-59 days
- Supply chain
- DDoS attacks are on the rise for life science

Cyber Loss Curve

- Most risk averse clients insure between the 95th-97th percentile.
- MPL for network outage, ransomware, data breach

Contractual Liability

- Damage caps of your top 10 customers
- Supply chain - reliance on complex vendors and global suppliers creates significant exposure. (delay, project loss, business interruption)

$1M is Inadequate

- Regardless of revenues or operating costs
- Ransom payment, computer forensics, restoration, breach counsel, business interruption, crisis management

SEC Cybersecurity Rules

On August 4, 2023, the SEC published rules that standardize and enhance disclosure of material cybersecurity incidents, risk management strategy, and governance by public companies.

Background:

With the pandemic came a decentralized workforce which resulted in widespread cyber attacks to both private and public organizations. The SEC recognized that oversight and regulation was needed as reliance on digitization and the escalation of cyber attacks posed a significant threat to business operations. In March of 2022, the SEC proposed cybersecurity recommendations for public companies related to increased disclosure and response. The revised rules by the SEC are a result of much discussion and debate over the proposed recommendations.

What Constitutes Materiality?

The likelihood that a reasonable person would consider it important when making an investment decision, or if it would significantly affect existing publicly available information about a company.

Key Requirements:

Event Disclosure – Company must disclose any material cybersecurity incident via Form 8-K within **4 business days of determining materiality**.

Risk Management Disclosure - Company must report their cyber security risk management strategy, including the process for managing cyber security threats, and whether any threats have materially impacted the company.

Oversight Disclosure - Governance (Form 10-K) Registrants must disclose their cybersecurity governance including oversight by the board and management.

Effective Dates:

December 12, 2023, for public companies: Form 8-K (if there has been a material cyber event)

June 15, 2024, for smaller reporting companies: Form 8-K (if there has been a material cyber event)

December 15, 2023 (fiscal year ending): Form 10-K (Annual reporting)

02

Management Liability Insurance

Convergence of Cyber and D&O Issues

Cybersecurity incidents can lead to securities class action litigation alleging management failed to maintain adequate measures to protect the company's data or failed to maintain adequate monitoring systems to detect security breaches

Heightened expectations around Board members having Cyber experience and around the Board's oversight on privacy issues

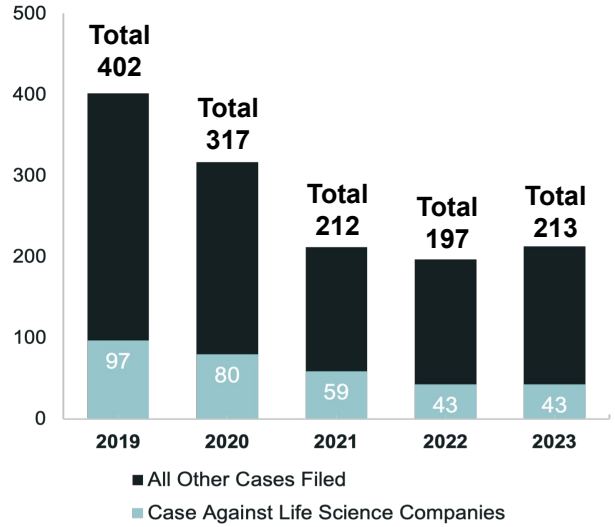
- ➔ Form 10-K disclosure

Increased accountability to the SEC

- ➔ Failure by CISOs to meet regulatory requirements can lead to SEC investigations, potential fines and reputational damage
- ➔ Is your CISO covered by your D&O policy?

Public Company D&O Claims Trends

Number of class action securities fraud cases filed from 2019-2023



Source: Dechert survey: Developments in Securities Fraud Class Actions Against U.S. Life Sciences Companies, 2023 Edition

Consistency in Filings

Securities class action lawsuit filings against life sciences companies were stable year-over-year at 43, though these filings were down over 50% compared to 2019.

Life science companies remained a popular target of securities class action lawsuits in 2023, accounting for nearly one in five total filings. Life sciences filings, as a percent of total, averaged nearly 26% from 2019 to 2021.

Claims Against Larger Companies

About 42% of life sciences companies named in complaints had market capitalizations of less than $500M in 2023 compared to nearly 60% in 2022, while around 23% of life sciences companies with complaints had market capitalizations of $5B or more versus approximately 16% in 2021 and 2022.

Plaintiff Law Firms

Four firms were associated with nearly half of the first filed complaints against life sciences companies: Pomerantz; Glancy, Prongay & Murray; Levi & Korsinsky; and The Law Offices of Frank R. Cruz.

Venue Trends Continue

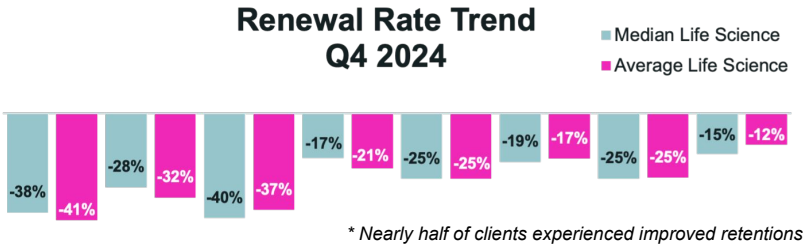
Consistent with historic trends, the majority of suits were filed in the Second, Third and Ninth Circuits. The Third Circuit experienced a 160% increase in filings in 2023 while the Ninth Circuit saw a 20% increase.

Allegations

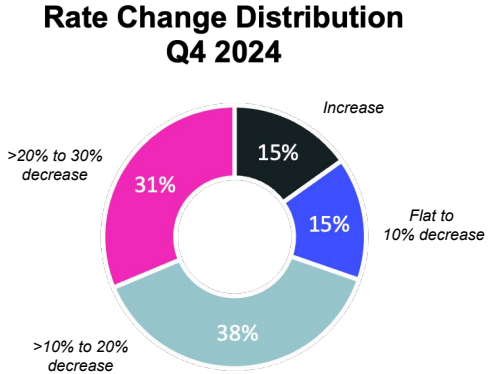
Allegation trends continued with misrepresentations regarding product efficacy and safety (47% of claims), misrepresentations involving regulatory hurdles (28%) and misrepresentations related to the company's financial reporting (35%) leading the way.

U.S. Public D&O Market Environment

Life Science Rate Trend



** Nearly half of clients experienced improved retentions*



Risk Profile

Publicly-traded clients are differentiated by claims history, financial condition, regulatory risk, market cap, class of business, and carrier relationship.

Favorable Conditions

Competitive capacity from new and legacy insurers drove material premium improvements beginning Q2 2022. Though premium reductions have tapered over the past year, we expect the pricing environment to stabilize but remain favorable with retention relief also possible.

Excess Layers

During the early stages of the current soft cycle, most clients experienced improving excess rates. Those rates have historically ranged from around 65% to 85%. With most excess rates currently near the low point of that range, excess layer premium outcomes will often mirror the primary result. Companies with challenging risk profiles may see excess rates at the high end of the range.

Outlook

Insurers are attempting to limit premiums reduction in 2025, so while Newfront expects the pricing environment to remain favorable, premium relief may be more measured than in the recent past.

D&O Takeaways for In-house Counsel

01	02	03	04	05
Get involved in the process	Be familiar with your policy before you have a claim	Ensure that you have appropriate limits	Thoughtfully select your insurers	Understand that D&O policies are not “off the shelf”

Employed Lawyers Liability Insurance

1

What is it?

Professional liability insurance to protect in-house attorneys against allegations of malpractice:

- Potential claimants include: creditors, customers, vendors, competitors, shareholders, employees, and government regulators (bar associations)
- Types of claims: negligent advice; defamation, breach of fiduciary duty, malicious prosecution.

2

Who is an Insured Person?

Employed lawyer is often defined as “any person admitted to practice law anywhere in the world who is, was or becomes a full-time or part-time employee of an Organization for the purpose of providing legal services to the Organization.”

Typically, coverage will extend beyond employed lawyers, to also include legal assistants/paralegals, as well as contract and temporary attorneys.

3

What does it cover?

When purchased on a standalone basis, coverage extends beyond legal services rendered to the employer, to include pro-bono activities, notary services, as well as moonlighting services.

4

What does it cost?

Relatively inexpensive (depending on size of legal department and limits purchased).

Can often be included as part of the D&O policy at no added cost, but there are potential drawbacks to this approach.

03

Top 10 Best Practice Insurance Management Processes

Other Coverage Considerations

Marine Cargo & Transit Coverage

- LMA 5403 Marine Cyber Endorsement excludes coverage for Malicious Acts
- Cargo carriers have developed specialized products to help close gap for previously uncovered cyber losses.
  - i.e. a temperature sensitive shipment of Drug Product spoiling because the logistics provider suffers a ransomware event while the product is in transit.

Products Liability

- Disclosure of Confidential Information is a typical exclusion on Life Science Products Liability policies.
- New Modular Products incl. Cyber being introduced to close gap for products that have combined Bodily Injury and Info Security Exposure
  - i.e. a pacemaker with internet connectivity capabilities

Clinical Trials Liability

- Sponsors of Clinical Studies very conscious not to identify trial participants, even in the scenario of a claim or serious adverse event that triggers insurance coverage.
  - Insurance carrier to work directly with investigators, brokers and patient directly to respond to claim without de-blinding the patient.
  - Important to have a broker that specializes in handling complex Life Science claims

Top 10 Best Practices for Risk & Insurance

1. **Engage your broker in strategic plans** including IPO, M&A, etc as there are insurance implications and also deal tools available such as RWI.
2. **Work with broker to create an informed plan around the local insurance requirements** for planned global clinical enrollment.
3. Launch **early renewal updates** and develop a **pre-renewal strategy** with broker.
4. Develop a **contractual review process of Indemnification and Insurance provisions of contracts** with your broker.
5. **Plan for claims** (IRP, tabletops, etc) to adhere with insurance policy terms and panel of resources.
6. **Avoid claims** – e.g. train entire employee population on recent phishing trends and build processes for out of band authentication (OOBA).
7. **Early reporting of claims**. engage broker following receipt of complaint to avoid undue friction or denials for late reporting.
8. **Proactively schedule quarterly risk & insurance reviews** with your broker.
9. **Monitor large capex investment and changes with supply chain in** CDMO's, CRO's, 3PL's, etc to make sure there is limit adequacy in StockThroughPut.
10. **Leverage technology** to make your job easier.

Q&A

Thank you

Eric Long | eric.long@newfront.com

Jennifer Wilson | jennifer.wilson@newfront.com

Branson Settle | brandon.settle@newfront.com

Dan Lindell | dan.lindell@newfront.com

Connect with our expert team to continue exploring insurance solutions for the life science industry