Lockton Cyber Marketplace Insights

Cyber & E&O Market Update – Q3 2024

CURRENT DYNAMICS

Current State

- Major market volatility has stabilized leading to a prolonged competitive cyber market
- Aggressive 2023 carrier growth goals & new market entrants created competition and drove premium decreases which have continued in 2024.
- Carrier experience & expertise is becoming more critical (longevity, claims handling expertise, risk management services, etc.)
- Insureds are faced with decisions to uproot incumbent relationships to achieve short-term premium relief that may, or may not foster a stable, consistent, long-term program
- Carrier concerns around systemic cyber risk and the evolving privacy regulatory landscape are impacting coverage offerings

Claims Landscape

- Significant/severe losses were experienced throughout 2023 and have continued in 2024. This will likely deteriorate carrier profitability and impact cyber market conditions.
- Over the past 18+ months, there has been a wave of class action lawsuits and privacy litigation arising from the use of Tracking Technologies & handling of consumer data by organizations

Emerging Coverage Considerations

- Evolving contractual liability exposures are changing the risk profiles of organizations
- Risk assessments should be conducted for Professional Liability and Technology E&O exposures arising out of an organization's products/services

Underwriting Requirements

- ✓ Minimum security standards still must be evidenced to maintain coverage efficacy and secure renewal capacity
- ✓ Security requirements are a moving target given the evolving threat landscape and new attack vectors being exploited

Global Growth Market

- Munich Re estimates that the premium in the global cyber market will grow from $14B in 2023 to $29B by 2027

KEY FACTORS

Actuarial Modeling

+ Cyber criminals and technology dependence create ever-changing exposures which inherently make pricing/modeling cyber insurance products elusive
+ Executing a Cyber-As-A-Peril strategy will enable long-term success

Underwriting Capacity

+ Carriers continue to monitor capacity deployment across their books of business. Aggregation events (actual & potential) are driving this focus
+ New market entrants and capital investment have enabled new/additional capacity to enter the marketplace

Rate Environment

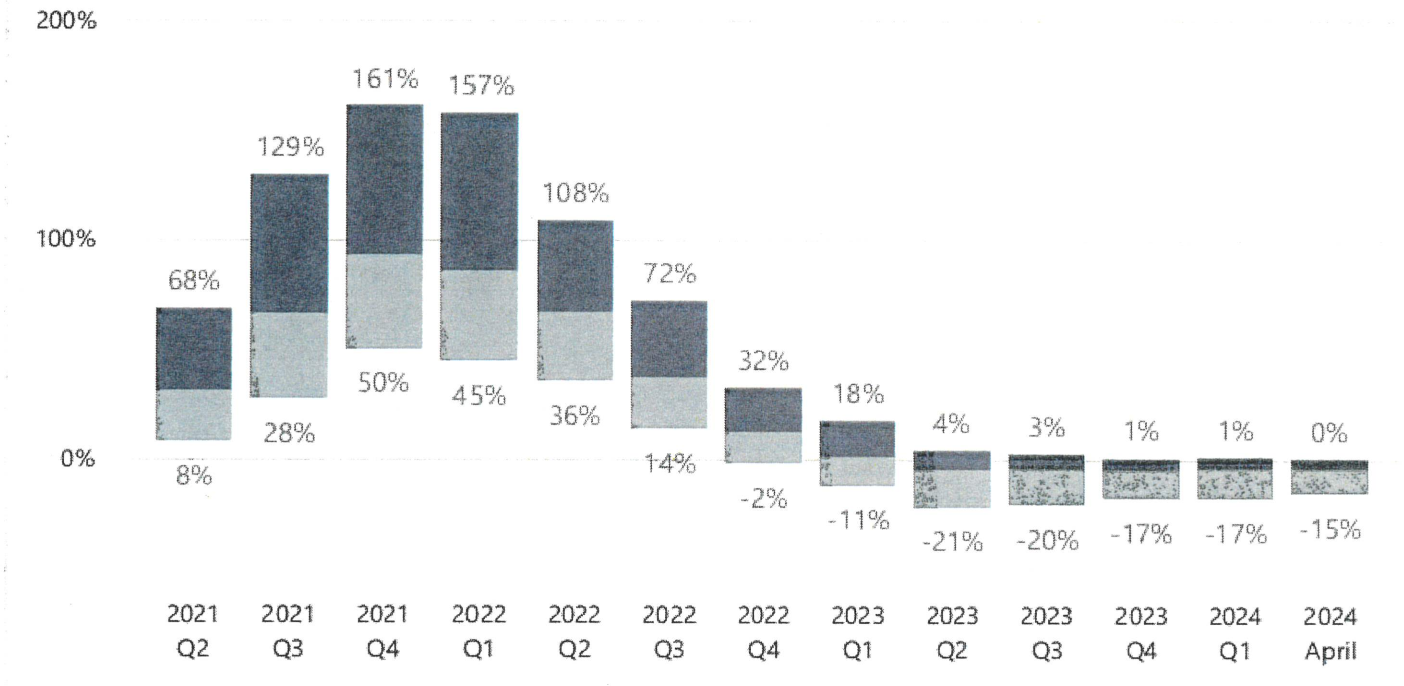
+ Market competition has led to premium decreases and pricing correlation in carriers offering coverage options
+ We anticipate the cyber rate environment to be fluid/dynamic as we navigate 2024

Coverage

+ Privacy regulatory coverage offerings/triggers are being scrutinized by carriers
+ Due to aggregation concerns, Dependent Business Interruption sublimits are becoming more common and limited to IT providers traditionally
+ War & Infrastructure exclusions are focal point for all carriers

Cyber Renewal Insights – Total Price Change

TOTAL PRICE CHANGE BY QUARTER



Quarter	Median	Average	Count
2021 Q2	31.6%	48.1%	370
2021 Q3	66.2%	101.1%	386
2021 Q4	93.5%	125.5%	422
2022 Q1	86.1%	124.1%	370
2022 Q2	67.1%	99.4%	420
2022 Q3	37.3%	52.7%	492
2022 Q4	12.9%	19.9%	593
2023 Q1	1.7%	6.4%	451
2023 Q2	-4.8%	-7.5%	533
2023 Q3	-4.3%	-6.4%	584
2023 Q4	-5.0%	-6.1%	659
2024 Q1	-4.3%	-5.5%	488
2024 April	-4.0%	-6.7%	68

25th-50th Percentile 50th-75th Percentile

Percentages displayed represent the 25th and 75th percentiles.

Source: *Policy renewal analytics on Lockton's book*

Lockton Cyber Renewal Insights

CURRENT DYNAMICS

Premium/Rate Changes

- Q1-2024 Average decrease: **-5.5%**
- Q1-2024 Median decrease: **-4.3%**
- April 1st renewals experienced decreases through the competitive marketplace:
  - Average decrease: **-6.7%**
  - Median decrease: **-4.0%**
- Q1-2024 Average price change (*increase or decrease*) by revenue size:
  - <$50M – **-4.0%**
  - $50M to $99M – **-5.3%**
  - $100M to $249M – **-6.6%**
  - $250M to $999M – **-5.4%**
  - >$1B – **-7.9%**

Other Insights – [1/1/2024 – 4/1/2024]

- Capacity trends
  - 12% of clients increased total limit at renewal, 1% decreased limit
  - 6% of clients that previously held $15M+ in total limit increased limit at renewal
- Retention
  - 8% of renewals experienced an *increase to retention*
  - 13% of renewals experienced a *decrease to retention*
- Coinsurance
  - 2% of renewals required *coinsurance*

UNCOMMONLY INDEPENDENT

Regulatory Landscape

International, federal, state and local regulators continue to expand privacy protections around the globe. Significant regulatory activity includes:

- European Union's General Data Protection Regulation
- China's Personal Information Protection Law and Data Security Law
- U.S. Treasury's Office of Foreign Assets control's updated advisory on ransomware payments
- State legislation, including:
  - California Consumer Privacy Act and California Privacy Rights Act
  - Virginia Consumer Data Protection Act
  - Colorado Privacy Act
  - Utah Consumer Privacy Act

Some laws have been around for some time but have recently seen an increase in litigation and/or enforcement activity. Examples include:

- Health Information Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Illinois Biometric Information Privacy Act (BIPA)
- Children's Online Privacy Protection Act (COPPA)
- Fair and Accurate Credit Transactions Act
- Regulation S-P
- Video Privacy Protection Act (VPPA)
- Federal and state wiretap laws

❖ As we are beginning to see ransomware attacks pick up again, the next wave/concern of cyber insurance carriers are with regards to the enforcement and resulting fines/penalties from privacy litigation. of Given the novelty of privacy laws, the frequency and severity of enforcement remains to be seen across the landscape.

❖ Many cyber insurance policies do not intend to provide coverage for privacy fines/penalties, unless they are resulting from a cyber breach. This is an area we will want to continue to discuss with regards to coverage at upcoming renewals.

Pixels

Article Link: Addressing the hidden privacy risk of 'tracking pixels' | Lockton

- Law firms, regulators and insurers are beginning to turn their attention to privacy risks created by tracking pixels collecting user data. For businesses regularly deploying cookies on websites or using tracking pixels, it's vital to have in place a transparent governance process to avoid facing legal action or regulatory intervention.
- A tracking pixel is a very small and often invisible image containing computer code that captures information. It differs from a cookie in that it is neither placed in a browser nor does it rely on a browser to function. Instead, it's usually placed on a website. Consequently, tracking pixels allow businesses to collect a wider variety of user information including email opens, digital ad impressions, sales conversions, website visits, and other types of online activity. In a recent move, the Austrian Data Protection Authority (DSB) has declared(opens a new window) that Facebook's tracking pixel violates the EU General Data Protection Regulation (GDPR) and the latest European Court of Justice (CJEU) decision on transatlantic data flows. Organizations subject to GDPR are required to obtain consent before tracking the online activities of individuals. Otherwise, they may face regulatory investigations and fines. With the above regulatory advance in mind, the risk of lawsuits and regulatory investigations related to the use of tracking pixels is clearly on the rise. While the urgency is more evident for industries that collect sensitive personal data, all organizations catering for the end consumer should be paying attention.
- Businesses deploying tracking pixels may face legal action claiming that the responsible party allowed the tracking company to intercept private communications – the interaction between the website and the individual – which plaintiffs say they never consented to.

To reduce the risk of attracting the attention of regulators and claimants, businesses deploying tracking pixels should consider the following actions:

- **Know your third-party tracking situation:** Determine what cookies, pixels and other tracking technologies are actually running on your website.
- **Consider limiting third-party tracking on the most sensitive portions of your webpage**: You know your websites and what website audiences care about. Consider whether to trim or eliminate third-party trackers from pages that arguably disclose more personal information or allow sensitive inferences to be drawn.
- **Prune unnecessary third-party trackers**: Take inventory of your digital domain – be sure that all your tracking technologies have a clear and necessary purpose.
- **Give consumers a choice**: This can include the following, some or all of which may be required in some jurisdictions:
  - •Letting website users opt out of all third-party tracking for analytics and advertising purposes;
  - •Providing that choice before any third-party trackers are deployed; and
  - •Only dropping cookies for analytics and advertising purposes if consumers opt in affirmatively at the cookie banner or with the preference tool.
- **Use in-tool privacy choices to minimize the privacy impact of third-party trackers:** Most third-party trackers provide the organizations using them with the power to limit data collection. For example, a switch in the controls may allow a website operator to anonymize IP addresses that are collected, making it more difficult for a third-party service provider to identify a website user. If your company does not need the tracker to collect certain information, set the controls accordingly.
- **Disclose third-party tracking:** It is clear from the above that of the most rigorous disclosure will be required to ease concerns from data protection authorities and protect against potential future legal action. This can include the following, some or all of which may be required in some jurisdictions:
  - •A generic disclosure of use of tracking technology in a privacy policy;
  - •A listing of specific third parties doing the tracking, and for what purposes, in a privacy policy;
  - •A cookie banner disclosing deployment of cookies, pixels, and other third-party technology, with links to learn more; and
  - •A just-in-time disclosure in connection with capturing keystrokes