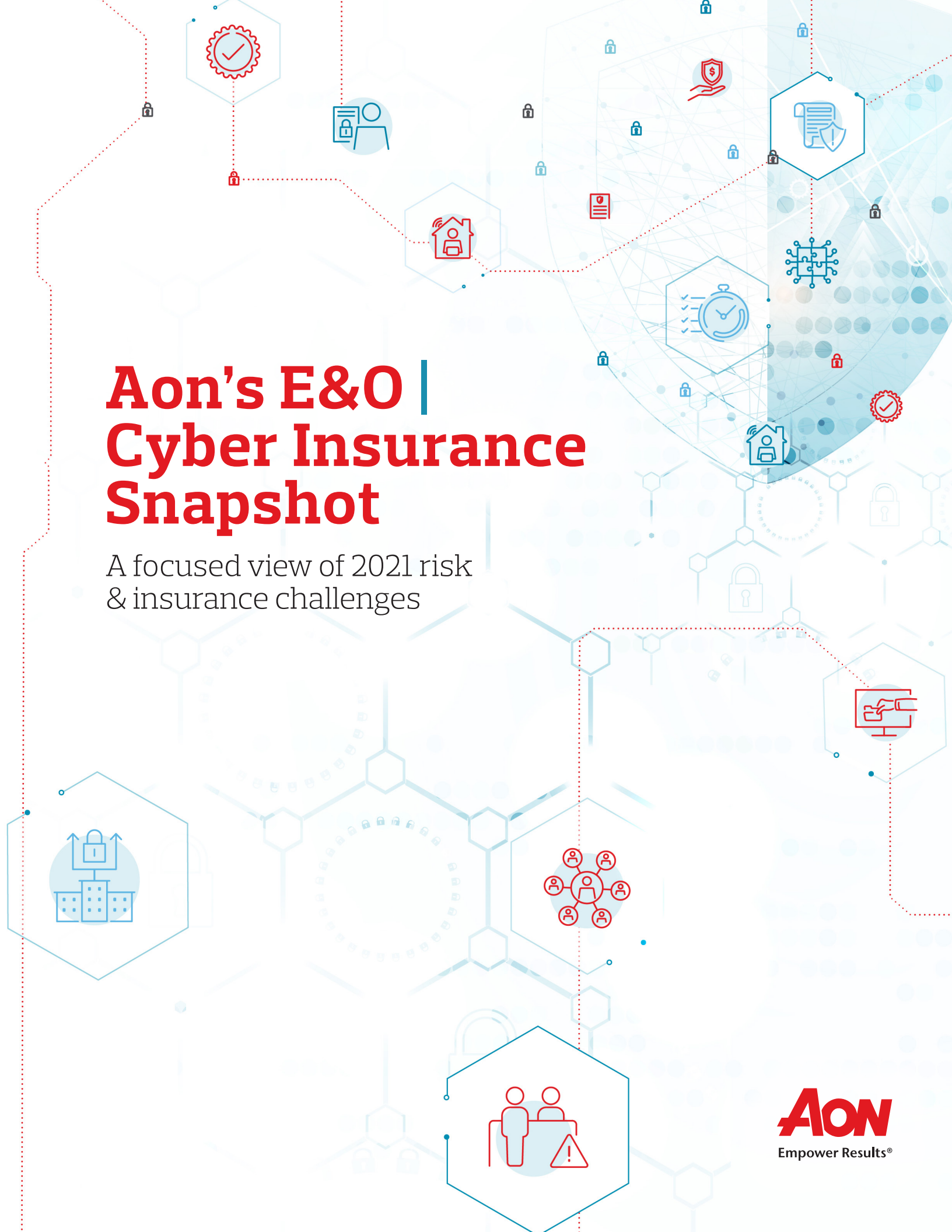
Aon's E&O | Cyber Insurance Snapshot

A focused view of 2021 risk & insurance challenges



Aon
Empower Results®

Aon's E&O | Cyber Insurance Snapshot

A focused view of 2021 risk & insurance challenges

In 2021, we expect a year of fluid market dynamics across the Errors & Omissions (E&O) and Cyber insurance product segments. As we help clients navigate a hard market cycle, we recognize the need to be proactive on renewal placements given a more diligent underwriting process, as well as the need to consider coverage options and creative program structures to help meet risk transfer objectives.

Throughout 2020, insurance carriers reached, and in many instances surpassed, a tipping point as loss frequency and severity outpaced improved risk selection and limited rate increases. E&O (including Media Liability, Miscellaneous Professional Liability (MPL), and Technology E&O) claim frequency and severity remained within assumed ranges during 2020, as did complex Cyber losses in the large/multinational client segment. The change that's been developing since late 2018, and ultimately tipped the scale in 2020, relates to ransomware activity across all revenue segments, but primarily in the Middle Market space.

Key 2020 trends include:

Claim Frequency - Aon's Cyber Solutions saw a typical cadence of three new E&O/Cyber matters per business day in 2020, **up almost 100%** from full year 2019, the majority being ransomware event-related.

Claim Severity - The average loss severity climbed each quarter of 2020. In many instances, **clients experienced eight-figure ransomware event-related losses**. Also, many of those large matters continue to be adjusted over the course of a year, as subsequent business interruption losses are reviewed, and liability claims are litigated.

Pricing - While average pricing increased from 2019 to 2020 by 5% –10%, guidance from almost all insurers has been that those rate adjustments were not enough to compensate for the **increase in frequency and severity of losses**.

Risk Selection - Insurers bolstered supplemental tools throughout 2020. Some carriers are using public-facing scanning resources to search for vulnerabilities that could be subject to cyber threats, and many have introduced new ransomware specific applications. These efforts are focused on **improving insured risk controls**, as well as **improving risk selection for insurers**.

We anticipate all these trends will continue throughout 2021, at an accelerated pace. Aon's Cyber Solutions has received guidance from some of the largest insurers in the product segment that we should **anticipate 20%–50% rate increases throughout 2021**. To maintain a commitment to long-term stable cyber capacity, insurers are reviewing areas in their portfolios where underwriting action is needed, and **reevaluating capacity deployment, specifically as it relates to ransomware losses**.

Our goal as we provide a snapshot of the 2021 E&O/Cyber insurance marketplace is to support our clients by bringing context to the challenges—both quantitative and qualitative—that insurers are trying to manage; share data on historical pricing trends paired with forward looking guidance offered by insurers that support these products; and prepare clients as they approach the market in what is likely to be the most challenging year to date in the history of E&O/Cyber coverage.

Risk Trends to Watch

Uncovered Technology Errors & Omissions (E&O)

COVID-19 has accelerated digital transformation initiatives for many organizations. The emergence of technology services and product exposures in more traditional industries represents a potentially "new" E&O exposure that may not be contemplated by existing insurance.

Remote Workforce

The remote workforce is here to stay, increasing potential vulnerabilities given Remote Desktop Protocol (RDP) software, remote access security, reliance on third party IT service providers, and digital communication as the primary venue to share information.

Breach Regulations

The regulatory environment continues to grow in complexity on a state, national and global basis. Recent fines under the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Regulation (CCPA) and the Illinois Biometric Information Protection Regulation (BIPA), demonstrate that organizations should be mindful of the impact of a breach. Continued evolution in this space could bring larger financial concerns from a fines and penalties standpoint.

Cyber Extortion

Theft and misuse of personally identifiable information (PII) is no longer the golden goose of bad actors. Ransomware attacks have evolved to include not only the encryption of sensitive data (including PII and confidential corporate information), but also the threat of exposure of sensitive data on the public Internet. These types of attacks may result in corporate downtime due to encrypted networks as well as potential liability consequences in terms of regulatory fines or third-party lawsuits.

Vendor Risk

As organizations continue to adapt to the current business environment and associated market needs, reliance on third-party technology and back-end applications has never been higher. Supplier cyber security standards are a critical part of this equation. The recent SolarWinds compromise demonstrates the complexity of technology supplier relationships and how they may potentially add risks that may impact cyber security posture.

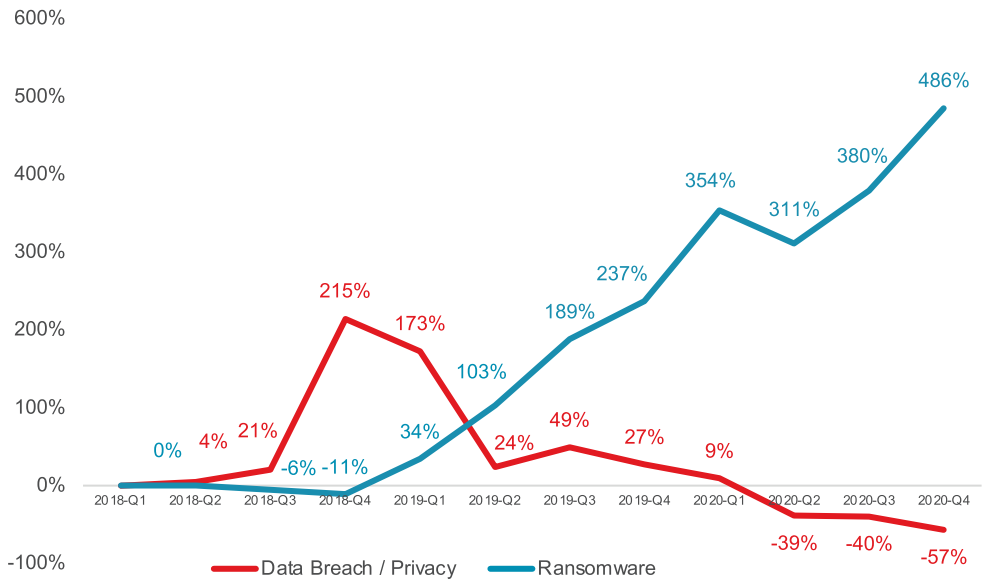
Loss Trends

Cyber Incident Rates Over the Past 12 Quarters

(Percent change relative to 2018-Q1)

Key Observations:

- Ransomware activity has dramatically **outpaced Data Breach/Privacy Event activity over trailing four quarters**
- **Ransomware up 486%** from Q1 2018 to Q4 2020
- Aon's Cyber Claims intake indicates 2020 will show a compounding **increase of 150%, +300% over trailing two years**
- Data Breach/Privacy Events tracking to decline in 2020, **first decline in trailing five years**

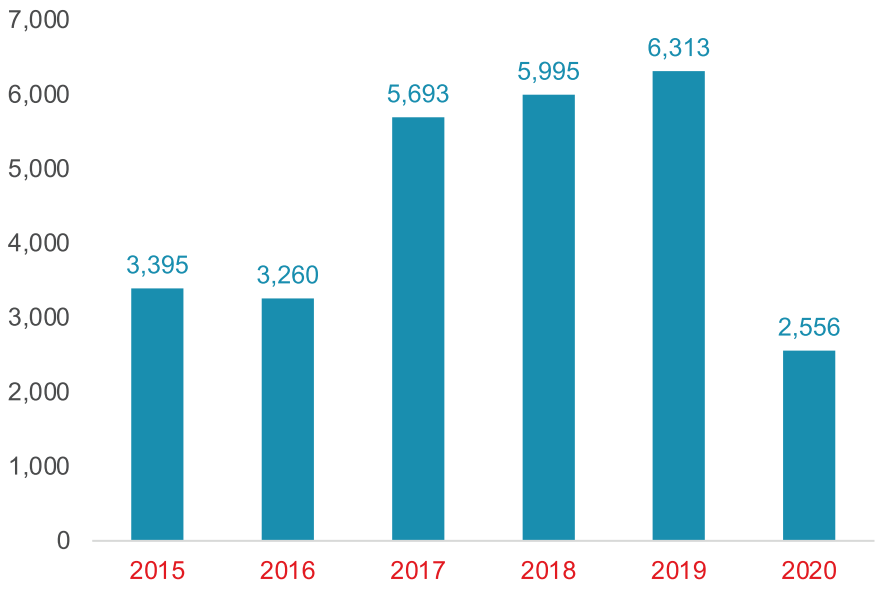


Source: Risk Based Security, analysis by Aon. Data as of 1/5/2021; Ransomware payment per Coveware Ransomware Report as of 11/4/2020

Data Breach / Privacy Events by Year

Key Commentary:

- Analysis completed includes review of **publicly disclosed events**
- A "Data Breach/Privacy Event" would typically be defined as a **disclosed event,** which may not incorporate ransomware activity or other events not reported publicly
- 2020 was down **~60% YOY**
- Aon's Cyber Claim intake aligns with analysis, showing a **40% – 50% decline** in "Data Breach/Privacy Events"
- Aon's Cyber Claim intake is showing **~150% increase** in ransomware related matters in **1H 2020 vs. 1H 2019**



Source: Risk Based Security, analysis by Aon. Data as of 1/5/2021

Cyber Pricing Trends

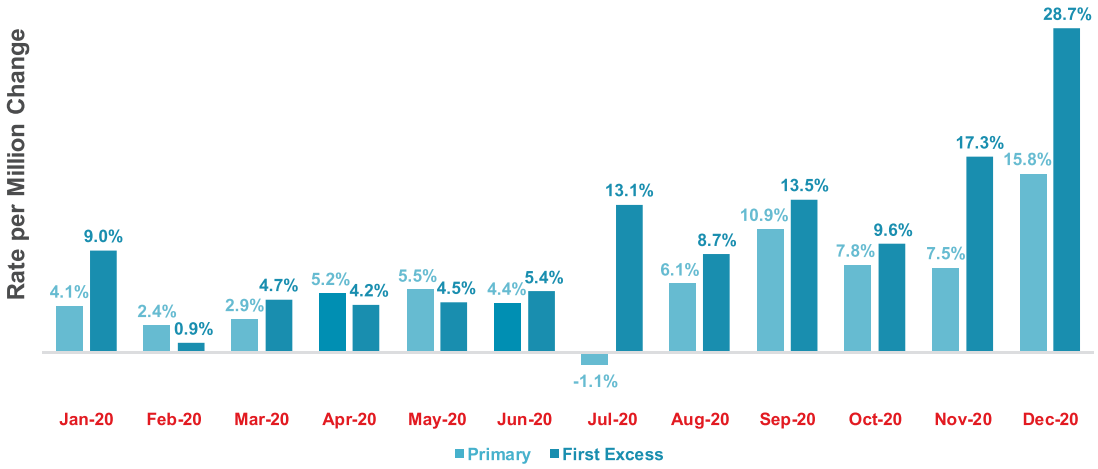
Cyber Pricing Changes – Primary and First Excess Only

Average Year-over-Year Change (Same Clients/Same Limits/Same Deductibles or Attachment Points)

Key Commentary:

For Cyber placements, clients saw single digit increases throughout much of 2020. The end of the year marked the turn to hard market conditions, with double-digit increases on both primary and first excess layers. First excess layers have tended to see greater increases than primary layers likely due to:

- Low excess capacity has historically been priced using competitive increased limit factors
- Given the increase in loss frequency and severity, larger cyber claims may erode the primary layer and impact the first excess layer
- Many insurers are managing overall profitability based on losses impacting their full portfolio



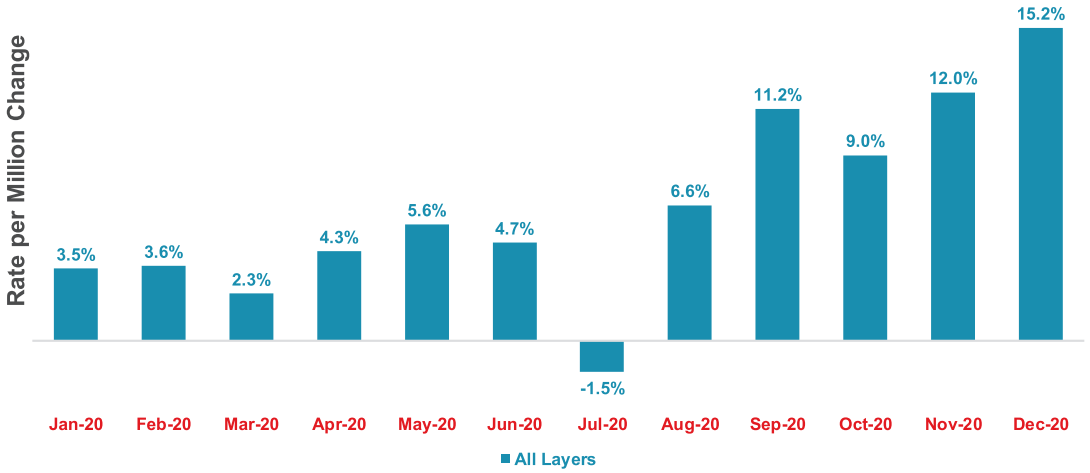
Source: Aon's Cyber Solutions Quarterly Pricing Index

Cyber Pricing Changes – All Layers

Average Year-over-Year Change (Same Clients/Same Limits/Same Deductibles)

Key Commentary:

For Cyber placements, program towers have shown rate increases transitioning from single to double-digits over the course of 2020. This is likely due to portfolio-wide pricing corrections, as well as macro-level insurer corrections due to economic challenges.



Source: Aon's Cyber Solutions Quarterly Pricing Index

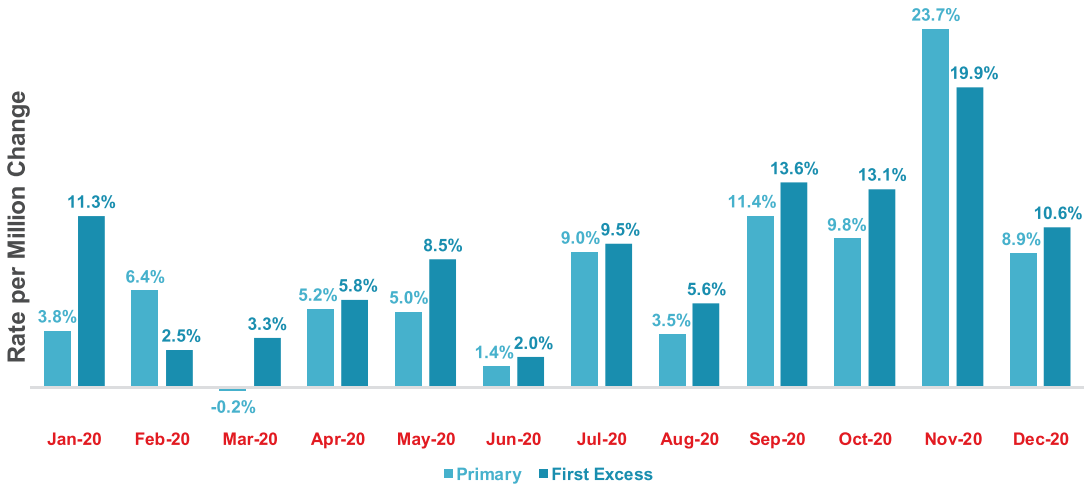
E&O (Media Liability, Miscellaneous Professional Liability, Technology E&O) Pricing

Monthly E&O Pricing Changes – Primary and First Excess Only

Average Year-over-Year Change (Same Clients/Same Limits/Same Deductibles or Attachment Points)

Key Commentary:

For E&O placements, clients saw increases on both the primary and first excess layers throughout 2020, due to continued frequency and severity of professional liability losses.



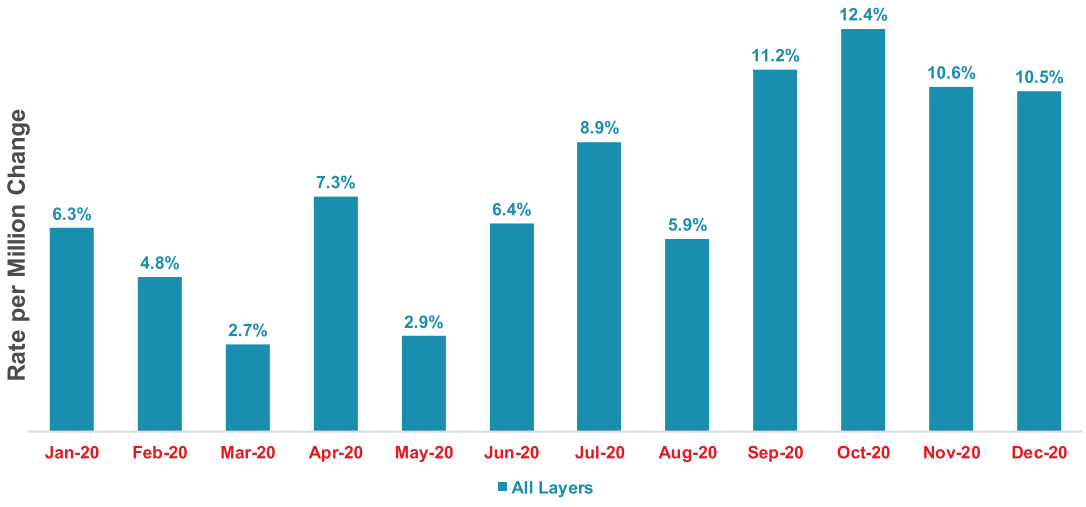
Source: Aon's Cyber Solutions Quarterly Pricing Index

Monthly E&O Pricing Changes – All Layers

Average Year-over-Year Change (Same Clients/Same Limits/Same Deductibles)

Key Commentary:

For E&O placements, program towers transitioned from single digit increases during the first half of the year, to double-digit increases starting in September 2020 for the balance of the year. This is likely due to portfolio-wide pricing corrections, and macro-level insurer corrections due to economic challenges.



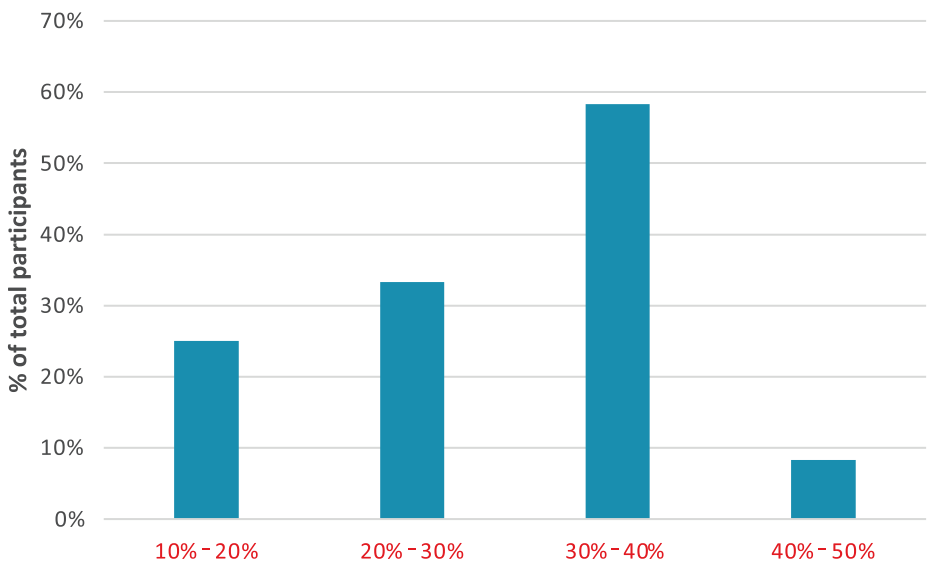
Source: Aon's Cyber Solutions Quarterly Pricing Index

Forward Looking Guidance

Forward Looking Rate Guidance

Aon releases a quarterly survey to the top 12 underwriters in the E&O/Cyber space. Below are some key pricing dynamics being felt throughout 2021:

- 58% of respondents suggested they are seeking rate increases **greater than 30% throughout Q2 2021**
- Historical pricing suggests an average PPM change of **0% – 10% throughout 2020**, with more substantial increases realized in Q4
- This information is based on an Insurer's overall rate targets for their portfolio. Each insured has a slightly different risk profile. It's important to represent to insurers how a particular Insured is best prepared to manage its own E&O/Cyber risks
- No insurers that responded suggested rate would be less than 10% YOY going in to Q2 2021
- **Aon anticipates pricing to be fluid throughout 2021**



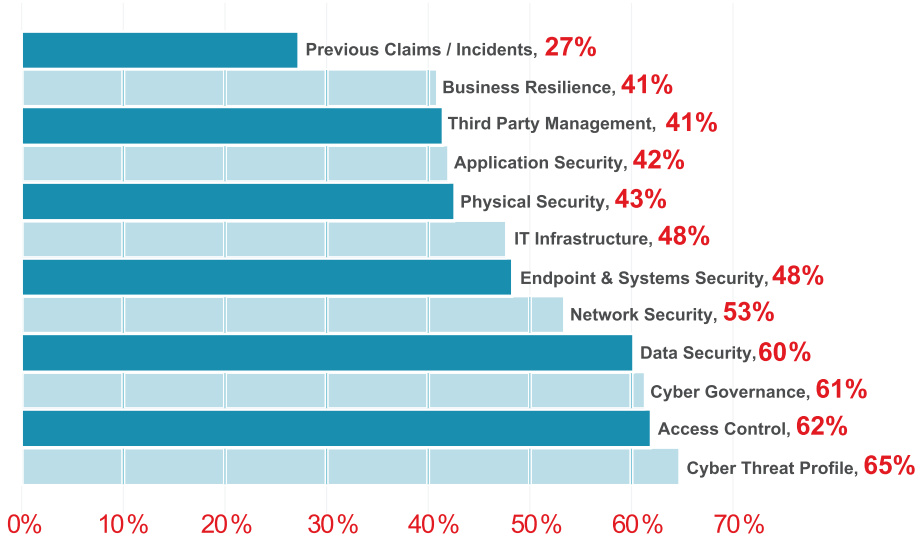
*Guidance is provided through Aon's proprietary survey of the top 12 E&O/Cyber insurers Aon trades with. This is not proposed pricing, or guidance specific to a particular insured's program. This is portfolio level guidance offered by underwriters who participated in the survey.

Source: Aon's Cyber Solutions U.S. Underwriter Survey, January 2021

Key Underwriting Topics

Key Commentary on Underwriting Topics:

- These topics are based on guidance from insurers on a forward-looking basis. They are ranked based on criticality to the underwriting process, however this list is by no means limited to these topics alone and should be considered a starting point for underwriting discussions based on specific industry and company exposures.



Source: Aon's Cyber Solutions U.S. Underwriter Survey, October 2020

Coverage Considerations

In response to the risk and loss trends described previously, insurers are adjusting their underwriting approach, reviewing terms and conditions of coverage, and reevaluating capacity deployment. The following are specific examples of coverage considerations that insureds will need to navigate in 2021.

Notice Requirements

Notice provisions remain an omnipresent and important consideration for professional liability policyholders, particularly as technology E&O exposures continue to increase for many insureds that were not traditionally providers of professional services. Understanding the distinction between "claims made" and "claims made and reported" notice provisions may be critical as late notice is among one of the most common causes of claims friction under E&O policies. Further complicating matters is the occasional inclusion of "occurrence" terminology within "claims made" and "claims made and reported" notice language, particularly with respect to technology failures or security issues that give rise to professional liability claims. The inclusion of such "occurrence" parlance does not in and of itself convert these policies to "occurrence"-based forms, further underscoring the need for insureds to understand the various nuances of notice obligations under their policy.

Dependent Business Interruption

The SolarWinds compromise has caused insurers to review their overall exposure to systemic, aggregated, correlated risks, related to the software supply chain. The breadth of coverage afforded for business interruption losses is being reviewed by several insurers with a specific mind toward limiting the financial exposure to a systemic event in the following ways:

- Reconsidering waiting periods. In many cases, waiting periods had been negotiated to between six and eight hours (and in some instances removed entirely). The marketplace is beginning to push for waiting periods closer to 24 hours, such as those seen in the Property marketplace.
- Limiting aggregate limit exposure. This is being achieved through the reintroduction of sub-limits or requirement of coinsurance.

Ransomware Event Coverage

Ransomware events and their associated losses are cited by many insurers as a major factor impacting their cyber insurance loss ratios. Should appropriate underwriting information not be provided, or if the information provided is viewed unfavorably, insurers may seek to limit their coverage for ransomware event losses.

- Several insurers are moving to a limit deployment strategy where they may cap the total aggregate limit they offer to any insured to some factor of the total policy limit. Coinsurance is also being proposed, in some cases, in conjunction with a sub-limit.
- Waiting periods are being reviewed for the business interruption insuring agreements related to ransomware events, again in some cases being as high as 24 hours.
- In the most extreme cases, where critical controls are lacking, insurers may seek to include "ransomware event" exclusions to policies.

It is critical to note that while insurers are using these approaches to limit their exposure, these coverage restrictions are not designed to only apply to a ransomware or cyber extortion insuring agreement. Rather, the restriction is written such that it applies to ransomware as an attack vector (a "ransomware event"), and hence may limit coverage for any loss that would arise from such an attack.

Breach Response Vendors

As loss ratios deteriorate, insurers are closely reviewing third-party vendor costs incurred to investigate and respond to cyber incidents. To reduce (or at least combat the increase in) these costs, insurers are demonstrating less flexibility in the use of non-panel or pre-agreed vendors.

In addition to more challenges related to the use of non-panel vendors — particularly if there was no discussion/vetting of the vendor before the vendor's engagement for an incident — insurers are making fewer exceptions related to vendor rates. It is becoming increasingly common for insurers to only reimburse an amount equal to what the insurer would have paid a panel vendor.

Be a Better Risk – Recommendations

With the shift to a hard insurance market at the close of 2020, a strategic approach to policy placement is critical. Beginning the renewal process early, in terms of meeting with key underwriters, focusing on existing carrier relationships, and determining current renewal appetite may mitigate surprises.

FOCUS ON: Cyber Security

While no organization can eliminate the threat of a breach, being able to demonstrate basic steps to reduce the risk and significantly decrease the impact of a threat actor is critical. This requires proactive risk mitigation strategies including assessment, testing and practice improvement. It also requires incident response readiness, including conducting table top exercises and proactively retaining key third-party incident response providers. Leveraging resources available through an organization's insurer partners may improve the outcome should a loss arise.

FOCUS ON: Privacy

Privacy maturity may be demonstrated via established and updated policies that address third-party contracts, online presence, service providers, supply chains, and each business unit. Emerging privacy regulations and requirements should be routinely reviewed with counsel, and insurance language should be reviewed to ensure it is broad enough to meet the evolving environment.

FOCUS ON: Cyber Security Culture

Employee cyber security and phishing training can demonstrate a culture of cyber security. No longer is this just an Admin/IT/Finance problem, employees should be trained to work to combat malicious actors and reduce common vulnerabilities. Without demonstrating adequate security training, insurers may struggle to provide competitive coverage terms or premium pricing.

FOCUS ON: Ransomware & Business Interruption

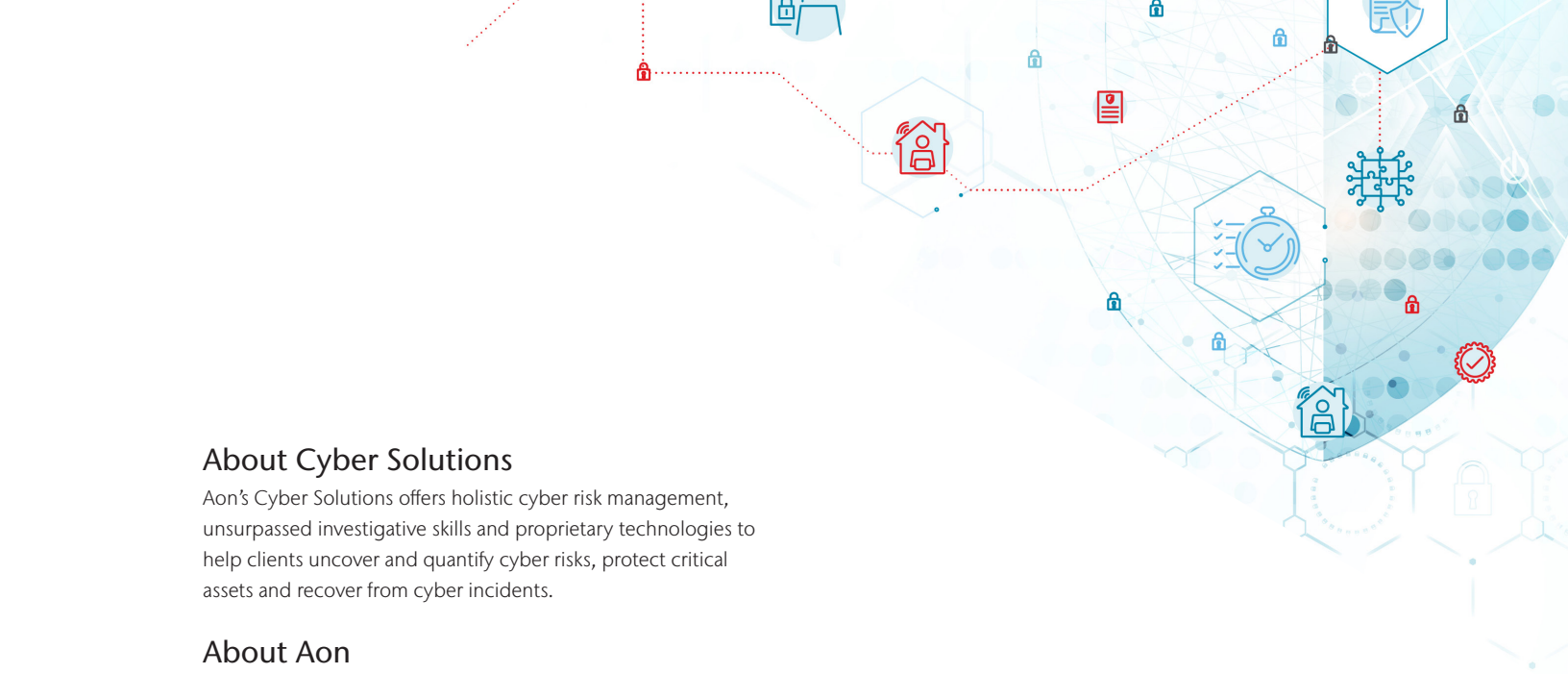
With carriers seeing both an increase in frequency and severity of ransomware-related losses, companies should be prepared to showcase preparedness for a ransomware attack. Insurers are reviewing this exposure via specific questionnaires and use of scanning technology. Focus is on business continuity/ disaster recovery planning, privileged access controls, multi-factor authentication, proactive scanning/ testing, and overall incident response readiness. This attack vector is of utmost concern to underwriters and will continue to transform the insurance market for the next several years.

FOCUS ON: Contracts

Third-party contracts are of consideration from a technology supply chain and contingent/dependent business standpoint. Considering the recent SolarWinds compromise, these critical supply chain and IT vendors are at heightened risk for "single point of failure" hacks impacting multiple organizations. It is critical to understand how both contracts and insurance respond in the case of a supply chain security breach.

FOCUS ON: Insurer Transparency and Communication

As E&O risks grow in complexity, it is important not only to ensure primary carrier engagement relative to coverage terms and conditions, but also to ensure excess carrier understanding of the primary policy provisions. Additionally, it is prudent to review exclusions that could come from other insurance lines such as Crime, Property, Casualty and General Liability. Maintaining a clear and transparent relationship with both primary and excess insurers may better inform policy intent and improve claim outcomes.



About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit **aon.com/cyber-solutions** for more information.

Empower Results®