RISKPOINT
INSURANCE ADVISORS

What to Expect with Your Cyber Insurance Renewals

RISKPOINT
INSURANCE ADVISORS

As you have probably heard, the cyber market is continuing to harden as we move further into 2021. In the first quarter, various industry sources reported rates went up between 18% and 25%, while some firms encountered renewals as high as 100% to 500!

Besides increasing rates, some carriers are lowering sub-limits for cyber extortion and/or including a co-insurance requirement while others are tightening their underwriting of the social engineering (cybercrime) exposure or withdrawing from specific classes altogether.

Industry pundits expect increases to continue at the same rate or higher as the industry cyber loss ratio exceeded 100% for the first time in 2020 driven by increasingly frequent and higher ransomware demands. As cyber claims hit the headlines weekly, our experience at RiskPoint mimics the national trends. We are seeing both Ransomware and Social Engineering claims and loss amounts are skyrocketing, with many of the claims exceeding seven figure payouts.

The good news about cyber, unlike other liability lines is that claims can be adjusted in fairly short time periods. This partly explains why rates have been going up so quickly as underwriters can almost watch their losses develop in real time instead of over many years. While this causes short term pain, I am hopeful it also means we may find some rate stability fairly soon as rates begin to match the current loss environment.

However, the best way for the rates to stabilize is for insureds to take their cyber security seriously to prevent the onslaught of ransomware and social engineering attacks. Businesses that take proactive preventative measures, will be insurable. Businesses that do not will find coverage unavailable or significantly restricted.

Businesses that take proactive preventative measures, will be insurable.

RISKPOINT
INSURANCE ADVISORS

Market Survey

We recently surveyed 25 cyber carriers and all but three are requiring Multi-Factor Authentication (MFA) on all new and renewal accounts. The handful making exceptions are doing so on small business risks or risks with other cyber security controls in place.

To prepare to obtain cyber coverage, we have compiled a list of minimum cyber security measures most carriers now require or will require in the near future.

We recently shared the attached MFA article explaining and highlighting the need for MFA and Endpoint Detection and Response (EDR). Most carriers responding to our survey also noted that they require receipt of a ransomware application prior to binding if such wording was not already built into their application.

The implementation of the security controls below will meet most of the security requirements the underwriters are looking for in their ransomware applications. As a caution, many carriers are voiding their quotes if they find the below measures are not in place prior to binding so it is recommended to confirm all subjectivities are met prior to making any binding request.

To improve cyber underwriting results, many carriers are using external cyber security scans of computer networks, finding the use of technology a far more effective underwriting tool than paper applications.

Minimum Recommended Security Measures

- **Multi-factor authentication** protection on **all remote access** to your network (including any remote desktop protocol connections), email server, cloud services and data backup solutions.
- **Multi-factor authentication** protection on **all network administrator accounts** and any other user accounts with elevated permissions within your network.
- A robust b**ackup solution that is either disconnected ("air-gapped") from your network or segregated from your network** with multi-factor authentication access control. Backups should be **tested frequently** and, ideally, be capable of restoring essential functions within 24 hours in the event of a wide-spread ransomware attack across your network. **All backups must be encrypted and it is recommended there be at least 3 backups created and stored separately. Ideally, two physically and one on the cloud**.

Minimum Recommended Security Measures Continued

- **Next-Generation anti-virus protection**, including automated **behavioral-based Endpoint Detection & Response** software functionality, on all endpoints. All detected suspicious **endpoint activity should be monitored & investigated 24/7/365**. Endpoints are the physical endpoints of a network such as laptops, mobile phones, tablets, servers and virtual environments.
- An **email filtering solution** that pre-screens emails for potentially malicious attachments and links. If using Office 365, we strongly recommend enabling the Microsoft Advanced Threat Protection add-on.

Renewal Preparation

- Communicate with your IT team and let them know that they will need to be involved in the application process and to respond thoroughly and quickly.
- Be prepared for longer applications with more questions and requirements to bind coverage.
- Return your application timely.
- Expect an increase in premiums and possible carrier changes.

We have several tools and strategies to assist in risk management, so if you have questions, please do not hesitate to contact our team.