SAMPLE UNDERWRITING QUESTIONS

In this guide, we share SAMPLE ransomware & multi-factor authentication questions that are being asked by carriers. These questions can be used as a sample of items the underwriters are using to evaluate and rate policies.

As we see ransomware threats increase at an alarming rate, taking proactive measures to ensure the best outcome at renewal becomes essential.

What is Ransomware? It is a type of malware that employs encryption to hold the victim's data. The bad actor then threatens to expose that data or holds it ransom in the pursuit of a payout.

What you need to know:

Insurance policies can provide coverage for the ransom pay out or negotiation costs under the 1st-party coverage of a cyber policy. That coverage grant is known as extortion or cyber threat.

Carriers are much more cautious now when underwriting new and existing accounts. This is in part due to large breaches, such as Solar Winds, C N A, T-Mobile and the Colonial Pipeline cyberattacks. What's being asked of the applicant is above and beyond anything we've seen before. Carriers are now requiring supplemental questionnaires in order to offer coverage and Multi-Authentication Factor (MAF) questions have become very important in their decision-making process. Answers considered unfavorable can lead to reduction of limit, reduction of coverage grants, or non-renewals.

What can you do?

A suggested best practice is for the broker and client to review sample ransomware and multi-factor authentication questions during the mid-term meeting to bring to light the underwriter's expectations at renewal time. The intent is to help clients understand what the carriers are looking for and where they can begin to either prepare or take action to mitigate their cyber risks. It is also a best practice to review current market conditions as a basis of setting the stage for what is likely to be a premium increase at renewal based on the current trends in the market.

Following are sample questions compiled from several carriers to assist you with your preparation.

- Does insured provide security awareness training to employees? How often?
- Does insured utilize simulated phishing attacks to test employee awareness? Is a third party utilized? Are corrective measures taken for employees that fail the test?
- Does the insured have a document process to report suspicious emails?
- Does the insured use web-filtering to block known malicious websites?
- Does the insured require authentication for employees remoting accessing the corporate network? Please address tactic (VPCN, Cloud-based email or CRM?) Is remote desktop protocol (RDP) enabled? Is RDP encrypted?
- Is multifactor authentication required for all employees? For Email? Systems? VPN? Cloud services? Data in Transit? Data at Rest?
- Is multifactor authentication contractually required for Independent contractors and/or vendors accessing the insured's network or cloud-based services? What is the estimated percentage required?
- Does the insured utilize antivirus? Endpoint Security tools with behavioral detection?
- Does the insured have dedicated staff to monitor security operations 24/7? Is this outsourced?
- How many employees have administrator access?
- Does the insured engage in annual penetration testing?
- Does the insured monitor the network with SIEM (security information & event monitoring) tools? Monitor traffic for suspicious transfers of data? Monitor storage capacity issues? Utilize a tool for monitoring data loss?
- Does the insured have a written process for end-of-life products or retired software?
- Are there written patch management procedures in place?
- What backups do the insured use? Onsite, offsite or in the cloud? Are they segmented? How long does it take to access?
- What backups do the insured use? Onsite, offsite or in the cloud? Are they segmented? How long does it take to access?
- Does the insured have a documented plan to respond to a ransomware or extortion event?
- Does the insured have a documented plan to respond to a third party vendor or customer's ransomware or extortion event?
- Has the insured established bifurcation or compartmentalization to all for "kill chain" segmentation?

- Does the applicant have a policy that all portable devices use full disk encryption?
- How quickly are critical patches deployed? 24-72 hours? 3-7 days? 7 days?
- Is there a process of creating backups? Documented or ad hoc?
- How often are backups made?
- Does the Applicant have a documented disaster recovery process?
- Does the Insured test its ability to restore critical systems and data in a timely fashion from its backups.
- What is the applicant's Recovery Time Objective (RTO) for its critical systems
- Does the applicant have a documented disaster recovery process?

HOW TO USE THIS GUIDE:

The incumbent carrier questionnaire should be reviewed between clients and their broker at mid-term. The intent is to help clients understand what the carriers are looking for and where they can begin to either prepare or take action to mitigate their cyber risks. If used as a map or guide for what to do in the 6 months before the renewal, this may save premium and time spent hunting excess tiers.