Executive Summary Cyber Liability:

BEAZLEY RENEWAL

The network security and privacy (cyber) liability program for DuPage County Government and Elected Officials expires on 12/1/23 with Beazley Insurance Company. The expiring program was bound with a $1,000,000 aggregate limit of liability with an additional 500,000 person limit for notifications and credit monitoring expenses, $500,000 for forensics and legal, and a further $1M for all breach responses costs (notifications, credit monitoring and forensic expenses) paid outside the limit of liability. There was a $1,000,000 (each claim) retention for a total annual premium of $170,000, or $176,078, including taxes/fees.

After a difficult few years, we were hoping for an easier renewal, despite the cyber market still being classed as "unstable". Ransomware claims have continued to litter the market, along with MetaPixel class action claims, and with that, underwriting scrutiny has increased further.

We're pleased to present that Beazley quoted a flat renewal, at $170,000 premium, with most terms, conditions as expiring. Further, after some strong negotiating and additional info from DuPage County Government and Elected Officials, Beazley were able to improve terms, offering increases to the following 1st party limits from $100,000 to $350,000: Cyber Extortion, Data Restoration, Business Interruption (both system failure and security failure) and Dependent Business Interruption (only security failure).

Due to underwriting changes at Beazley and reinsurance requirements, Beazley did add several new endorsements this year:

- MetaPixel/Tracking Exclusion
- Catastrophic Loss Exclusion (reduces limit to 50% on First Party losses)
- War and Cyber War Exclusion
- First Party Loss Exclusion Amendatory

ALTERNATIVE OPTIONS

Alliant did a thorough marketing as detailed in the summary below, knowing that the market had shifted since last renewal. We received alternative terms from three markets, Corvus, Travelers and Coalition, with the latter being the strongest. Coverages are summarized in the DuPage County Cyber Comparison document, and all premiums are detailed below: We recommend Coalition Option 2 below.

Corvus:

1. $1M limit in excess of $100,000 retention at $92,330 premium (excluding SLT)
2. $1M limit in excess of $150,000 retention at $87,745 (excluding SLT)
3. $2M limit in excess of $150,000 at $126,739 premium (excluding SLT)

Travelers:

1. $1M limit in excess of $100,000 retention at $93,154 premium (excluding SLT)
2. $2M limit in excess of $100,000 at $134,841 premium (excluding SLT)
3. $3M limit in excess of $150,000 at $165,440 premium (excluding SLT)

Coalition:

1. $1M limit in excess of $100,000 retention at $72,900 premium, $75,481 including all Surplus Lines Taxes and Fees
2. $3M limit in excess of $250,000 at $145,800 premium, $150,961 including all Surplus Lines Taxes & Fees
3. $5M limit in excess of $250,000 at $202,500 premium, $209,669 including all Surplus Lines Taxes & Fees

ALTERNATIVE OPTIONS, cont.

As is evident above, Coalition has the most competitive premiums and limit options. Two significant things of note which are highlighted in the comparison document:

- Coalition does provide a separate limit outside the limit of liability for Breach Response Services (forensics, legal, PR, etc). This limit is equal to the limit of liability quoted, so effectively doubles the total limit on offer.
- They do have a 50% coinsurance provision for ransomware at the moment. This can be removed with simple confirmation of the following: confirmation the applicant maintaining at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network, or in the cloud. We have Confirmed IT meets this and this 50% coinsurance for ransomware is removed.
- Coalition would like to offer this insured a Ransomware Tabletop Exercise; at no additional cost to them, which DuPage County will participate in.

  This exercise would consist of one of Coalition's Panel Vendors virtually meeting with the insured to go over various Ransomware Scenarios with the insured. This can be customized to the insured's preference (i.e. maybe more higher-lever overview if the CFO, CEO, etc are involved; or more in-depth if just the IT team attend the Tabletop Exercise).

Privacy Breach Response Services – these expenses do NOT erode the maximum aggregate limit

The Company will provide Privacy Breach Response Services to the Insured Organization, in excess of the Retention, because of an incident (or reasonable suspected incident) that first takes place on or after the Retroactive Date and before the end of the Policy Period and is discovered by the Insured and is reported to the Underwriters during the Policy Period. Services to include:

1. for an attorney to provide necessary legal advice to the Insured Organization to evaluate its obligations pursuant to Breach Notice Laws or a Merchant Services Agreement and in connection with providing the Breach Response Services described below;
2. for a computer security expert to determine the existence, cause and scope of an actual or reasonably suspected Data Breach, and if such Data Breach is actively in progress on the Insured
   Organization's Computer Systems, to assist in containing it;
3. for a PCI Forensic Investigator to investigate the existence and extent of an actual or reasonably suspected Data Breach involving payment card data and for a Qualified Security Assessor to certify and assist in attesting to the Insured Organization's PCI compliance, as required by a Merchant Services Agreement;
4. to notify those individuals whose Personally Identifiable Information was potentially impacted by a
   Data Breach exceeding the Notified Individuals Threshold;
5. to provide a call center to respond to inquiries about a Data Breach that exceeds the Notified Individuals Threshold;
6. to provide a credit monitoring, identity monitoring or other solution listed in the Information Packet to individuals whose Personally Identifiable Information was potentially impacted by a Data Breach exceeding the Notified Individuals Threshold; and
7. public relations and crisis management costs directly related to mitigating harm to the Insured Organization which are approved in advance by the Underwriters in their discretion.

First Party Loss

To indemnify the Insured Organization for:

1. Business Interruption Loss that the Insured Organization sustains as a result of a Security Breach or System Failure that the Insured first discovers during the Policy Period.
2. Dependent Business Loss that the Insured Organization sustains as a result of a Dependent Security Breach or a Dependent System Failure that the Insured first discovers during the Policy Period.
3. Cyber Extortion Loss that the Insured Organization incurs as a result of an Extortion Threat first made against the Insured Organization during the Policy Period.
4. Data Recovery Costs that the Insured Organization incurs as a direct result of a Security Breach that the Insured first discovers during the Policy Period.