What is Cyber Insurance?

An Overview of Coverage and Claims

PRESENTED BY:
Marcus Beverly
Alliant Insurance Services
SCORE Board Meeting
October 24, 2024

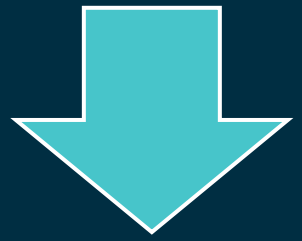
Agenda

- What is Cyber Exposure?
- Common Cyber Liability Coverages
- Who is at risk?
- Claim Examples
- Best Practices

What is Cyber Exposure?

Cyber exposures are directly connected to the responsibility an organization has for certain electronic information and the risks associated with this information being compromised or misused.

These risks include, but are not limited to privacy notifications, cyber extortion attacks, intellectual property infringement and financial injury, as well as obligations associated with Consumer Protection and Data Privacy Regulations.



First Party Risks

Third Party Risks

Alliant

Understanding Cyber Insurance

It's Data, Data Privacy and Computer Equipment Insurance

(First Party, Third Party and "Other")

First-Party

- **Protection for Loss of My Data**
- **Business Interruption From Unauthorized Access Which Affected My Computer or Data**
- **Protection for Damage to My Computer**

Third-Party

- **Liability For Losing Someone Else's Data**
- **Liability From Information Posted on My Website**
- **Government Fines for Not Complying to Specific Regulations**
- **Payment Card Fines For Non-Compliance**

"Other"

- Costs to Let People Know We Lost Their Data
- Costs to Have Help Understanding the Most Recent Data Privacy Laws in Every State and Internationally
- Costs to Have Help Navigating the Messaging to Put Forward
- Recovering Money Lost in a Fraudulent Email that Caused a Transfer of Money

Alliant

Common Cyber Liability Coverages

Breach Response

- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations/Crisis Management

First-Party

- Business Interruption
- Cyber Extortion
- Data Restoration
- eCrime
- Bricking
- Cryptojacking
- Reputation Loss
- Criminal Reward

Third-Party

- Data and Network Liability
- Regulatory
- Payment Card
- Media Liability

Alliant

Coverage Details: Breach Response

- Legal advice from attorney
- Computer security expert
- PCI forensics investigator
- Notification
- Call center
- Credit monitoring
- Public relations and crisis management

Coverage Details: First-Party – Business Interruption

- **Business Interruption Resulting from Security Breach**
- **Business Interruption Resulting from System Failure**
- **Dependent Business Loss Resulting from Dependent Security Breach**
- **Dependent Business Loss Resulting from Dependent System Failure**
  - Income loss
  - Forensic expenses
  - Extra expenses
  - Does not include unfavorable business conditions, loss of market or any consequential loss

Alliant

Coverage Details: First-Party

Cyber Extortion Loss

- Money, digital currency, marketable goods or services demanded to prevent or terminate an extortion threat

Data Recovery Costs

- Reasonable and necessary expenses to regain access to, replace or restore data

Fraudulent Instruction

- Transfer or payment of money or securities as a result of fraudulent written, electronic, or telephone instructions provided by a third party, that is intended to mislead through misrepresentation of a material fact

Funds Transfer Fraud

- Loss of money or securities in an account at a financial institution resulting from fraudulent written, electronic, or telephone instructions by a third party issued to a financial institution to pay or transfer money or securities without the insured's knowledge or consent

Telephone Fraud

- Unauthorized access to and using the Insured's telephone system by a third party

Criminal Reward

- Amount offered and paid for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to coverage under this policy

Alliant

Coverage Details: First-Party (cont'd)

Reputational Loss

- Reputation Loss that the Insured Organization sustains solely as a result of an Adverse Media Event that occurs during the Policy Period, concerning: a Data Breach, Security Breach, or Extortion Threat that the Insured first discovers during the Policy Period

Computer Hardware Replacement

- Reasonable and necessary expenses incurred by the Insured Organization during the Period of Restoration in a Business Interruption or Dependent Business Interruption loss to minimize, reduce or avoid Income Loss, over and above those expenses the Insured Organization would have incurred had no Security Breach, System Failure, Dependent Security Breach or Dependent System Failure occurred; which includes reasonable and necessary expenses incurred by the Insured Organization to replace computers or any associated devices or equipment operated by, and either owned by or leased to, the Insured Organization that are unable to function as intended due to corruption or destruction of software or firmware directly resulting from a Security Breach.

Invoice Manipulation

- Direct Net Loss resulting directly from the Insured Organization's inability to collect Payment for any goods, products or services after such goods, products or services have been transferred to a third party, as a result of Invoice Manipulation that the Insured first discovers during the Policy Period. Invoice Manipulation means the release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a Security Breach or a Data Breach.

Cryptojacking

- Direct financial loss sustained resulting from Cryptojacking that the Insured first discovers during the Policy Period. Cryptojacking means the Unauthorized Access or Use of Computer Systems to mine for Digital Currency that directly results in additional costs incurred by the Insured Organization for electricity, natural gas, oil, or internet

Alliant

Coverage Details: Third-Party

Data & Network Liability

Damages and claims expenses (legally obligated) on a claim for a data breach or security breach

Regulatory Defense & Penalties

Monetary civil fine or penalty payable to a governmental entity

Claims expenses

Payment Card Liabilities & Costs

Monetary amount owed under the terms of a merchant services agreement as a direct result of a data breach

Does not include charge backs, interchange fees, discount fees or other unrelated fees

Media Liability

Loss from an act committed in the course of creating, displaying, broadcasting, disseminating, or releasing electronic media material to the public

Coverage Details: Exclusions (Including But Not Limited To)

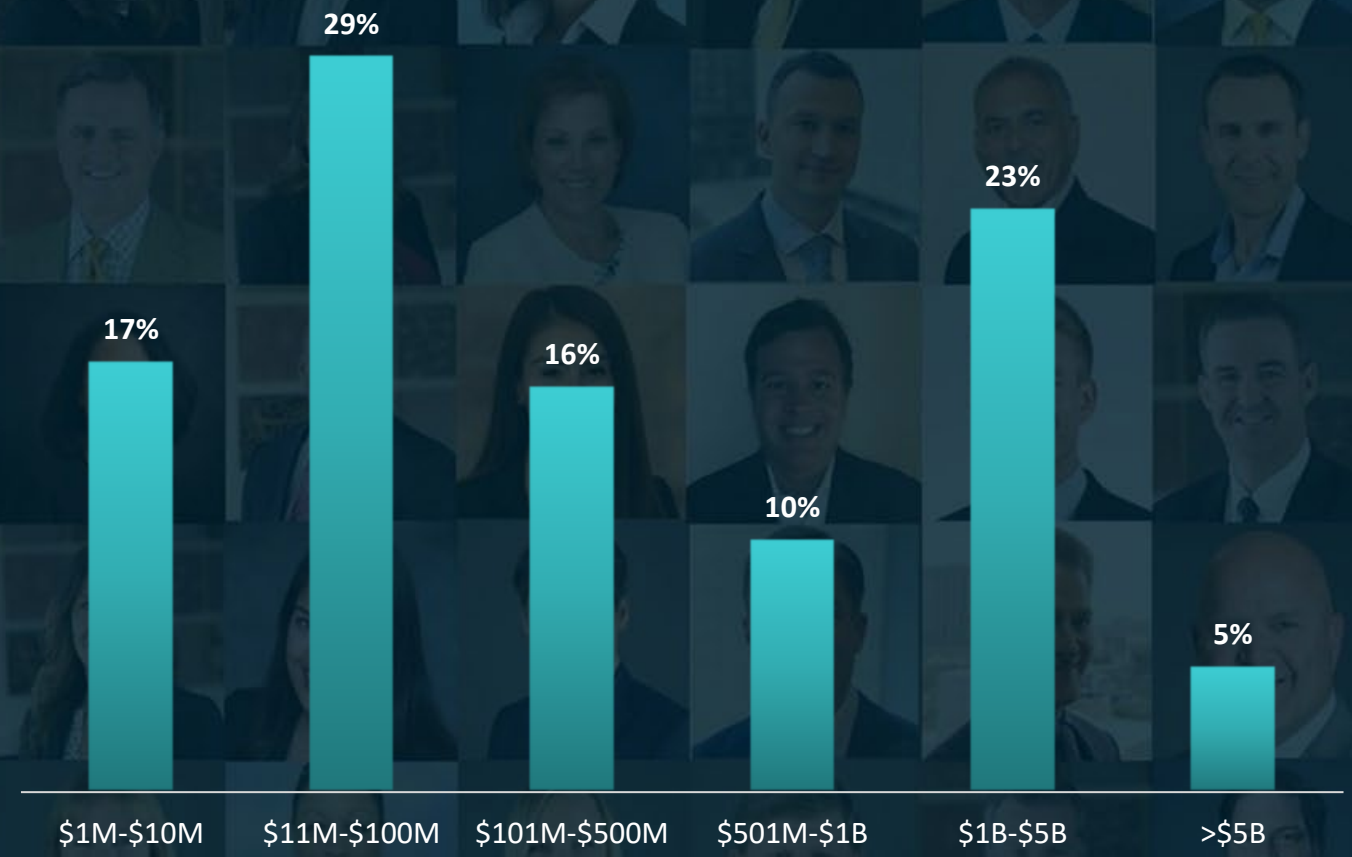
- Bodily Injury
- Property Damage (carve back for Bricking - computers or any associated devices or equipment)
- Insured vs. Insured
- Unlawful Collection of Personally Identifiable Data
- Prior Known Acts
- Betterment
- Failure of Power, Utility, Mechanical or Telecommunications Infrastructure or Services That are Not Under the Insured's Control

Alliant

Who is at risk?

Industries Affected

Cyber Attacks by Entity Annual Revenues



Source: BakerHostetler - 2023 Data Security Incident Response Report

Alliant

Industries Affected

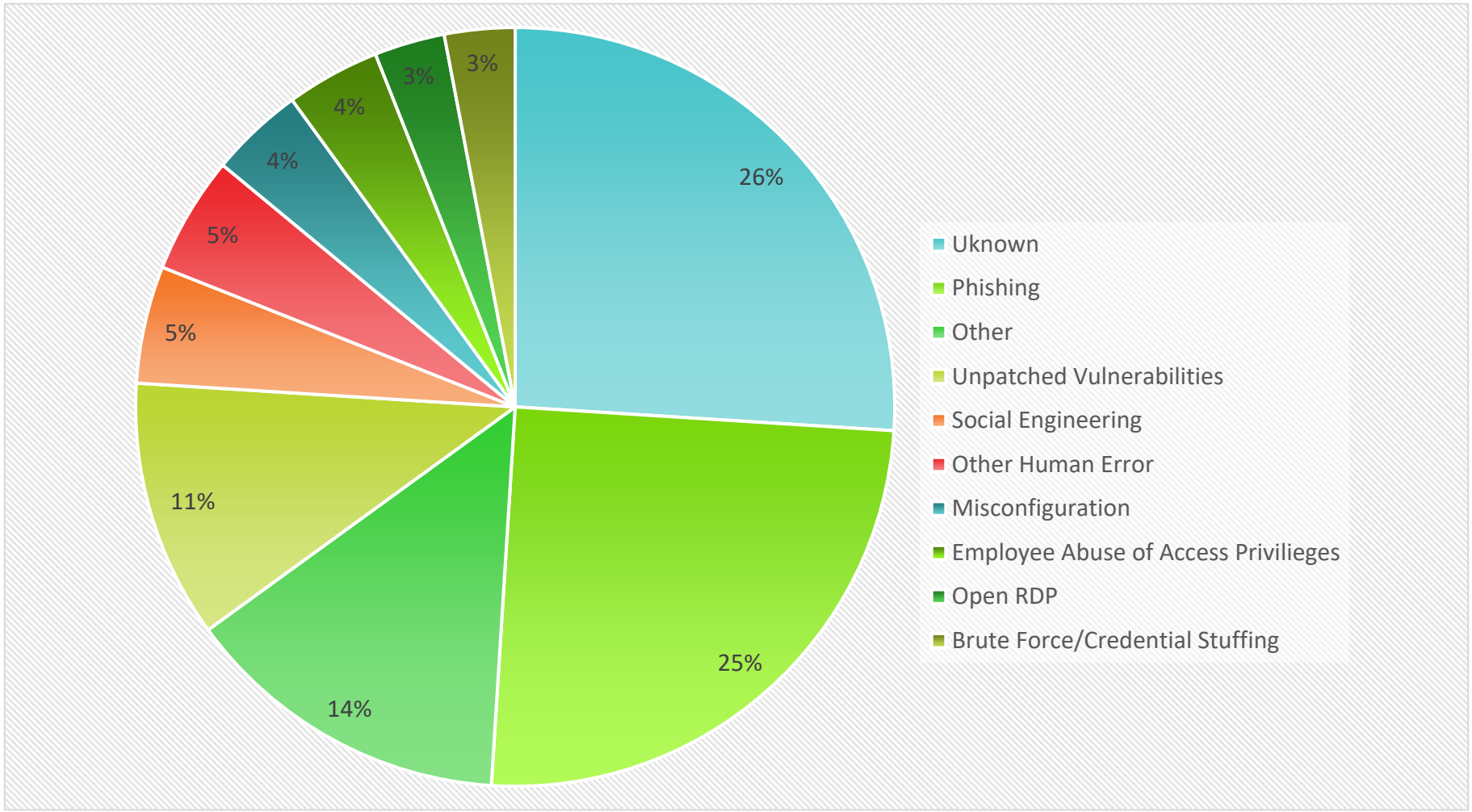
Data is listed in averages unless otherwise noted

	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
HEALTHCARE	**$3,257,688** (median: $1,475,000)	**$1,562,141** (median: $500,000)	**10.3** (median: 7)	**$73,781** (median: $30,000)	**71,370** (median: 696)
EDUCATION	**$1,791,650** (median: $750,000)	**$281,525** (median: $175,000)	**12** (median: 7)	**$68,695** (median: $53,000)	**9,567** (median: 415)
GOVERNMENT	**$1,069,120** (median: $500,000)	**$101,500** (median: $68,000)	**16.8** (median: 8)	**$100,293** (median: $23,750)	**19,701** (median: 2,004)

Source: BakerHostetler - 2023 Data Security Incident Response Report

Alliant

Why Do Incidents Occur?



Source: BakerHostetler - 2023 Data Security Incident Response Report

Alliant

Claim Examples

	Public Entity A	Public Entity B	Public Entity C
What Happened	A single lost unencrypted laptop	Ransomware Attack	Ransomware attack. Core clinical server, pharmacy, lab, electronic records all breached. Hospital system admins were able to quickly shut the systems down and restored most everything because of well-kept backups.
Coverage Parts Affected	100% Breach Response	Breach response as well as 3rd party claim for data network liability	Breach response as well as BI claim
Size of Claim	$383k Total $319k for doc review $50k for legal $14k notification costs 9k notified lives	$400k Total in breach response $300k for computer forensics $100k legal ??? For third party claim	$45k Total for breach response $20k legal $25k forensics $5M proof of loss submitted for BI
Lessons Learned	Make sure all workstations and mobile equipment are encrypted	Forensics revealed that no health data was breached so no notifications were required and the insured is facing a 3rd party class action suit regardless. Lesson is that healthcare faces the threat of a class action suit even if data is not breached.	Patient data was encrypted and wasn't accessed. 46 hospital employees had information accessed. Insureds want their money quickly after a claim but the larger and more complicated the claim is, the longer it will take.

Alliant

Claim Examples (cont'd)

Industry	Cause of Breach/Claim	Detail
Public Entity	Data Breach	A public entity suffered a security breach that took down all systems. The organization incurred substantial costs in response to the downtime and suffered significant data loss. Insurance carrier reviewed and adjusted the organization's proof of loss, paying over $190,000 in BI and data protection losses.
Public Entity	Hacking or Malware Cyber Extortion	A town government's computer systems were encrypted by a ransomware virus. All court records including police department records and administration records were encrypted. Insurance carrier connected the town with a vendor to help the town pay the ransom and decrypt the data. Because the ransomware did not have exfiltration capabilities, the town did not have to notify impacted individuals.
Education	Social Engineering Data Breach	A school district's HR department received a phishing email purporting to be the district's superintendent. Responding to the email's request, the HR department sent a pdf of all the district's employees W-2s to the emailer, thus releasing all the employees' tax information and Social Security numbers and putting them at risk of fraudulent tax filings as well as identity theft. Insurance carrier assisted the district by quickly connecting them with legal counsel, who helped them notify employees by email within 36 hours of the incident, and follow-up with a formal notification via mail. Insurance carrier also helped arrange for the mailing and subsequent call center, as well as obtaining credit monitoring resources for the impacted population.
Healthcare	Unintended Disclosure Data Breach	An IT vendor had inadvertently unsecured a file containing over 30,000 patients' billing information such that it was searchable on the internet using search engines such as Google. The hospital discovered the incident during security testing when a larger healthcare system acquired the hospital. The information exposed included names, social security numbers, date of births, addresses, treatment information, and insurance information. The hospital utilized outside legal, forensics, notification services, a call center, credit monitoring and crisis management. The hospital was investigated by OCR and four attorneys general.

Source: Beazley

Best Practices

- **Multi-factor authentication – 100% implemented for:**
  - Remote access (Faculty, Staff, and Students – not uncommon with Universities, not yet required for K-12 students)
  - Privileged access
- **Well managed end point detection and response**
- **Well managed RDP connections – VPN, MFA, etc.**
- **Back Ups**
  - 1 working copy, 1 offsite, disconnected not working, 1 onsite disconnected not working
  - Tested at least twice a year
  - Ability to bring up within 24-72 hours – less time for critical operations (4 hours)
  - Protected with antivirus or monitored on a continuous basis
  - Encryption
- **Planning and Training (and Frequency)**
  - Incident response plan / Business continuity plan
  - Social engineering training / Phishing training / General cyber security training
  - Training of accounting/finance staff on fraudulent transactions
- **Reasonable patching schedule/plan**
- **Plan or adequate measures in place to protect end of life software**
- **IT Security Budgets**
- **Email Security**
- **Identity Access Management**
- **Service Account Management**
- **Zero Trust Philosophy to Network Access**

Alliant

Reasons to Purchase Cyber Insurance

You Are Not a Hermit and Have Computers and Data

- Your organization relies on computer equipment and communication to operate, an outage could have wide reaching affects
- Your organization has yours and others data, damaged, stolen or loss data can affect your operations

Mitigate Risk – Typical Insurance Stuff

- You want to protect your financials
- You want to have a partner to help you out financially should a loss occur
- You want to manage your downside risk

Unfamiliar Territory and You Want Expert Help - FAST

- Organizations don't have the resources to keep up with all the new threats, once an incident occurs, you need someone who knows what to do immediately
- You want a trusted source to have vetted out the vendors you approach, as when you are the most vulnerable you need to know you can trust your business partners

No 100% Secure System – You Want To Do What You Can Now

- Even the FBI gets hacked. You want to plan as best you can incase you should have an unauthorized access to your system
- Part of the plan is risk mitigation and lining up cyber security expert partners

You Are the Expert in Your Field – Rely on Cyber Experts to Keep Current

- Your organization is good at what it does, and does not have the resources to dedicate to manage the constantly changing environment of cyber risks and solutions
- You rely on organizations who do this on a daily basis to provide you with the most up to date coverage and services to help you, should you ever need it

Alliant

CLAIMS NOTIFICATION AND RESPONSE PROCESS

Notifying Beazley of a Cyber Incident (1 of 2)

When?

ASAP!

Any suspected Data Breach, Security Breach, Cyber Extortion Threat, or System Failure

Build notice protocols into your IRP

Escalate systematic, reputational, and catastrophic incidents

Helps preserve members' rights under applicable Policy

Who?

NOTICE OF CLAIM:

- IMMEDIATE NOTICE must be made to Beazley NY of all potential claims and circumstances (assistance, and cooperation clause applies)
- Claim notification under this policy is to:

Beazley Group

Attn: TMB Claims Group

45 Rockefeller Plaza, 16th Floor

New York, NY 10111

bbr.claims@beazley.com

Alliant (via email: Elaine.Tizon@Alliant.com

And copy your Alliant Team

Alliant

Notifying Beazley of a Cyber Incident (2 of 2)

Content of Notice

Include

- Briefly describe incident
- Date of incident event (if known)
- Date of incident discovery
- Contact information of your Breach Coordinator

Exclude

- Specific Personally Identifiable Information (PII) and/or Protected Health Information (PHI)

Alliant

The First 24 Hours

Secure your IT systems

Mitigate

Try to preserve all evidence pertaining to the incident

- Memories fade
- Emails get lost or deleted

Coordinate

You will be contacted by a Beazley Cyber Claims Manager or our Coverage Counsel representative (in coordination with Alliant)

Conference call to discuss the incident and investigation

- <u>Attendees</u>
  - Your Breach Coordinator (mandatory)
  - Key IRT members (recommended)
  - Beazley or Coverage Counsel

Alliant

The Incident Response Process (1 of 4)

What to Expect

Beazley is here to help you:

- Provide guidance
- Arrange investigation and response services
- Access to Beazley's network of experts and service providers
  - Vetted
  - Favorable rates (helps maximize the benefits of your policy!)

Experts and Service Providers

Privacy Counsel

Digital Forensics

Notification, Call Centre, and Other Services

Alliant

The Incident Response Process (2 of 4)

- Privacy Counsel (*highly recommended*)
  - Specialized, trusted attorneys
  - Represent you throughout incident investigation
  - Advise on and help prepare notifications, if necessary, to:
    - Affected persons
    - Regulators
    - General public
- Law Firms Beazley Recommends for Members

BakerHostetler

www.bakerlaw.com
mskoller@bakerlaw.com

McDonald Hopkins
A business advisory and advocacy law firm®

www.mcdonaldhopkins.com
jgiszczak@mcdonaldhopkins.com

  - Should you reach out directly to one of these firms regarding an incident, please also send in notice to Beazley and Alliant

Alliant

The Incident Response Process (3 of 4)

- Digital Forensics (if needed)
  - Experts in computer network and data security systems
  - Beazley can help:
    - Identify a recommended vendor(s)
      - Specialization/expertise
      - Real-time capacity (ensures effective and efficient response)
    - Work with you to select and approve a scope of work tailored to the project
- Beazley Recommended Forensic Service Providers for Members

CRA Charles River Associates

www.crai.com
aobuchowski@crai.com

LMG SECURITY

www.LMGsecurity.com
ksprenger@lmgsecurity.com

Kroll

www.kroll.com
bdemonte@kroll.com (East Coast)
pierson.clair@kroll.com (West Coast)

  - You may want to discuss with your privacy counsel on contracting with additional breach response vendors, such as forensics
  - Should you reach out directly to one of these firms regarding an incident, please also send in notice to Beazley and Alliant

Alliant

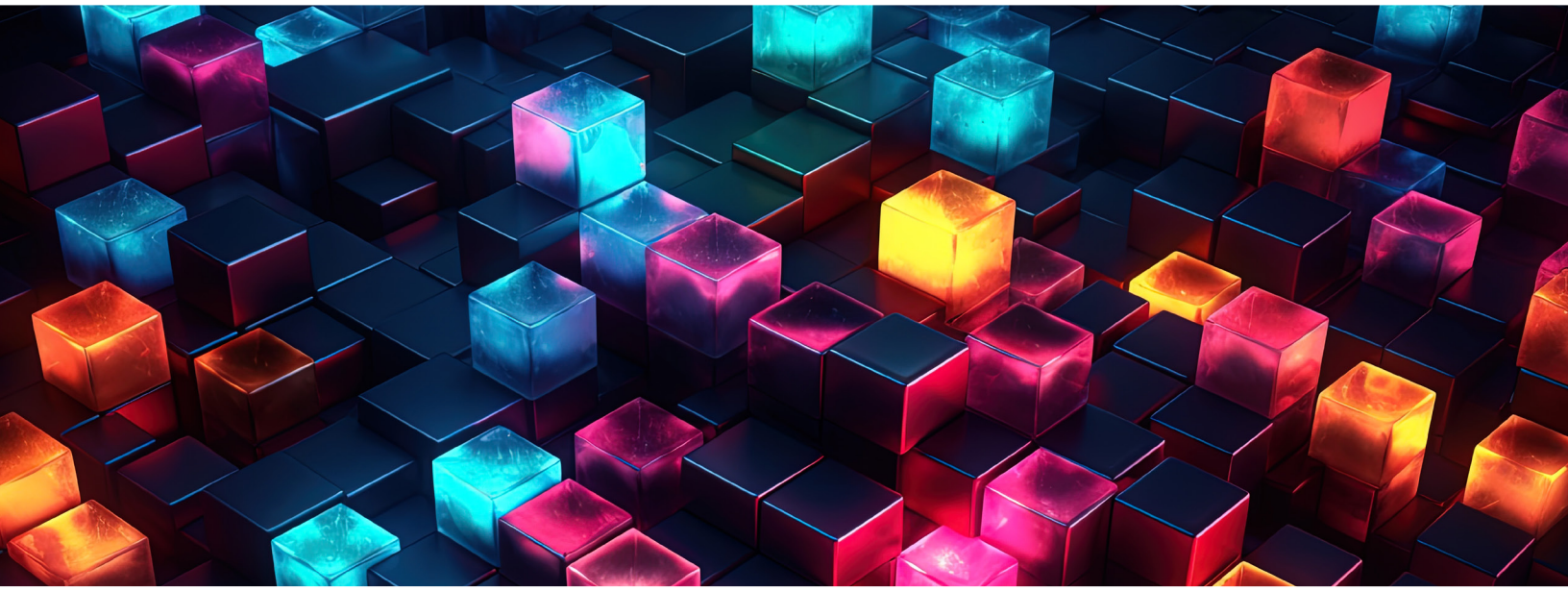
The Incident Response Process (4 of 4)

- Notification, Call Centre, and Other Services (if needed)
  - Fact of breach has been determined by forensics and privacy counsel

Offerings		
Print & Mailing	**Credit or Identity Monitoring**	**Public Relations**
Deliverables required of you: • Draft notification letters • Signature block • Organization's logo • Letterhead • Complete address file (using vendor's required format) • FAQs to train call center agents	Upon receipt of required deliverables, vendor will need 4-5 business days to process	Works closely with privacy counsel to: • Develop FAQs • Draft public statement • Help establish escalation procedures to guide the call center about when to redirect specified types of callers or sensitive topics to the appropriate internal personnel

Alliant

Thank you!



Cyber Resilience Services Subscription Bundle for APIP Clients

Alliant Cyber helps clients identify, evaluate, remediate, transfer and respond to the cyber risks that matter most to their organization, while driving better cyber risk management and insurability outcomes.

In order to help our clients achieve these objectives, Alliant Cyber is now offering this cost-effective bundled suite of Alliant Cyber Consulting services, driving better Cyber Resilience, Risk Management, & Insurability Outcomes for APIP Clients.

INTRODUCING THE ALLIANT CYBER RESILIENCE SERVICES BUNDLE!

WHAT IS IT, AND WHAT'S INCLUDED?

Cost-effective bundled suite of Alliant Cyber Consulting offerings, driving better Cyber Resilience, Risk Management, & Insurability Outcomes for APIP Clients.

CYBER INCIDENT TABLETOP & READINESS ASSESSMENT	SECURITY AWARENESS	THREAT & VULNERABILITY MANAGEMENT	VIRTUAL CYBER GUIDANCE	CYBER ASSESSMENT	CYBER REMEDIATION ASSISTANCE
Cyber Incident Tabletop Exercise & Readiness Assessment	Security Awareness Training	Threat & Vulnerability Monitoring Reports	CISO Advisory Assistance	Annual Cyber Insurability & Controls Assessment	Alliant Cyber Ecosystem

ALLIANT CYBER RESILIENCE SERVICES BUNDLE – *WHAT ARE THE SPECIFICS?*

EACH APIP CLIENT RECEIVES ACCESS TO THE FOLLOWING CYBER RESILIENCE SERVICES ON AN ANNUAL BASIS:

CYBER INCIDENT TABLETOP EXERCISE & INCIDENT RESPONSE READINESS ASSESSMENT

Alliant Cyber will host quarterly virtual Cyber Incident Tabletop Exercises, facilitated by senior leaders from Alliant Cyber, focusing on Cyber Threat & Incident Scenarios that are most relevant to APIP members Additionally, Alliant Cyber will perform an annual assessment of the each APIP member's existing Cyber Incident Response (IR) Plan measures.

QUARTERLY CYBER SECURITY AWARENESS TRAINING

Alliant Cyber will host and present foundational Cyber Security Awareness Training sessions, which may be attended by the organization's staff. Topics will include best practices and behaviors for preventing Cyber Incidents, in addition to an overview of key Threat considerations.

CISO ADVISORY ASSISTANCE

Alliant Cyber will provide "vCISO" strategic consulting guidance available on-demand, which will be delivered by Alliant Cyber's senior-most Cyber Consulting resources. Areas of focus for your organization can include inquiries related to cyber security strategy, priorities, controls, remediation, governance, compliance, and architecture.

QUARTERLY CYBER VULNERABILITY & THREAT REPORTS

Alliant Cyber will provide client with a quarterly summary of the organization's Cyber Vulnerability and Threat posture, with a focus on enabling the organization to mitigate and address any critical deficiencies.

ALLIANT CYBER ECOSYSTEM SERVICES

Alliant Cyber will provide access to all curated Cyber Security Services and Solutions via the Alliant Cyber Ecosystem. Through this service, Alliant Cyber can assist organizations in identifying optimal Cyber Security vendors and solutions, including unique bundled offerings and optimized pricing.

ANNUAL CYBER INSURABILITY & CONTROLS ASSESSMENT

Alliant Cyber will perform an accelerated and targeted assessment of the organization's current Cyber Security controls and Risk posture, in order to evaluate the organization's readiness for submission to the Cyber Insurance market. Focus will include the key controls and attributes that lead to an optimized Cyber Insurability outcome for the organization.

The above services are all included for a modest annual fee, ranging from $5,000 per year.

ALLIANT CYBER RESILIENCE SERVICES BUNDLE – WHAT'S IN IT FOR YOUR ORGANIZATION?

Cost effective and simple means to address key Cyber Security/ Insurability controls

Includes core "must-have" services, such as Cyber Incident Tabletop Exercises, Security Awareness Training and Vulnerability Management

Provides accelerated impact and value to Client's Cyber Risk Management & Security initiatives

Enhances insurability outcomes

OVERVIEW

- Subscription Service
- Can have a positive impact on Cyber Insurability outcomes
- Heavily discounted rate for services
- Enhances overall Cyber Risk Resilience
- All services are delivered by the Alliant Cyber Consulting team

BENEFITS

- Cost effective and simple means to address key Cyber Security/Insurability controls
- Includes core "must-have" services, such as Cyber Incident Tabletop Exercises, Security Awareness Training and Vulnerability Management
- Provides accelerated impact and value to Client's Cyber Risk Management & Security initiatives
- Enhances insurability outcomes

EACH APIP CLIENT RECEIVES ACCESS TO THE FOLLOWING CYBER RESILIENCE SERVICES ON AN ANNUAL BASIS

- Cyber Incident Tabletop Exercise & Incident Response Readiness Assessment
- Quarterly Cyber Security Awareness Training
- Quarterly Cyber Vulnerability & Threat Reports
- CISO Advisory Assistance
- Alliant Cyber Ecosystem Services
- Annual Cyber Insurability & Controls Assessment

FOR MORE INFORMATION, CONTACT:

CJ Dietzman, CISSP, CISA
Senior Vice President Alliant Cyber
Cell: 980-419-2145
cj.dietzman@alliant.com

ABOUT ALLIANT INSURANCE SERVICES

Alliant Insurance Services is the nation's leading specialty broker. In the face of increasing complexity, our approach is simple: hire the best people and invest extensively in the industries and clients we serve. We operate through national platforms to all specialties. We draw upon our resources from across the country, regardless of where the resource is located.

alliant.com | CA License No. 0C36861 © 2024 Alliant Insurance Services, Inc. All rights reserved.

CYGNVS Cyber Incident Command Center for Public Entities

From ransomware assaults to state-sponsored intrusions, cybercriminals exploit vulnerabilities embedded in the array of services local governments provide. The CYGNVS Cyber Incident Command Center enables Public Entities to plan, practice, respond and report to cyber incidents.

Tailored Defense for Public Entities—Seamless Collaboration with Your Team

CYGNVS converts static playbooks into dynamic response playbooks providing intuitive role-based access-controlled workflows. You can invite your internal and 3rd party teams and report to your stakeholders and regulators from one single pane of glass. Plus, you can use it even if your network is down and your files are encrypted.

Train How You Are Going to Fight

CYGNVS facilitates "training how you're going to fight" allowing public entities to practice their response plan against real-world cyber scenarios. This hands-on training approach ensures that response teams are well-prepared and aware of diverse cyber incidents targeting Public Entities. Ultimately this can help reduce response times and minimize the impact of cyber outages.

Secure Out-of-Band Collaboration

CYGNVS establishes a secure out-of-band incident response platform, creating an isolated environment for response efforts. Even if the primary network is compromised, CYGNVS ensures that incident response operations remain secure and unaffected, serving as a beacon guiding teams through the chaos of a cyber crisis.

Single Pane of Glass for Incident Management

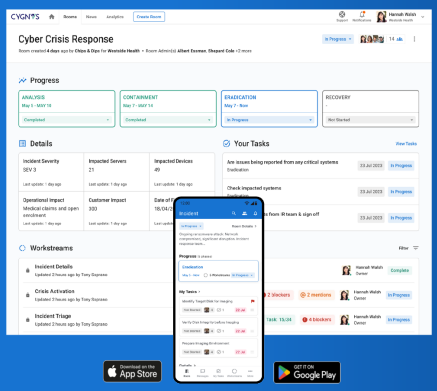
CYGNVS streamlines incident management by providing a single pane of glass for planning, practicing, responding, and reporting. This integrated approach ensures a comprehensive and coordinated response, reducing the risk of critical information slipping through the cracks and enhancing overall incident response efficiency.

Comprehensive Cyber Resilience with CYGNVS

Serving over 1,500 organizations around the world, the team of experts at CYGNVS has pooled together best practices from managing thousands of cyber incidents to build the CYGNVS Cyber Incident Command Center. The CYGNVS platform is designed for enterprise-grade security with SOC2 Type 2 compliance, ISO 27001 certification, and 24/7 live technical support. Learn more about how CYGNVS can help your organization plan, practice, respond and report during a cyber crisis by visiting www.cygnvs.com

CYGNVS helps prepare your organization to respond to the inevitable

- ✓ Secure, Out-of-Band Communications and Conferencing
- ✓ Fine-Grained Access Control and Data Retention for Internal Roles and External Providers



- ✓ SOC 2 Type 2 & ISO 27001; Multi-National, Multi-Lingual Response
- ✓ Library of Pre-Built Compliance Reports for 60 Jurisdictions

© 2024 CYGNVS All Rights Reserved.
DS1.2.27.24

US +1 650 684 2040 | EU/UK +44 20 8089 5851
INFO@CYGNVS.COM
4940 EL CAMINO, SUITE 100, LOS ALTOS, CA 94022

ALLIANT INSURANCE SERVICES, INC.
ALLIANT PROPERTY INSURANCE PROGRAM (APIP)

CYBER INSURANCE PROPOSAL
CORE COVERAGE

TYPE OF COVERAGE: Information Security & Privacy Insurance with Electronic Media Liability Coverage

PROGRAM: **Alliant Property Insurance Program (APIP) inclusive of Public Entity Property Insurance Program (PEPIP), and Hospital All Risk Property Program (HARPP)**

NAMED INSURED: APIP Cyber and Pollution Programs, Inc. which may include any member(s), entity(ies), agency(ies), organization(s), enterprise(s) and/or individual(s), attaching to each Declaration insured under the ALLIANT PROPERTY INSURANCE PROGRAM (APIP), inclusive of PUBLIC ENTITY PROPERTY INSURANCE PROGRAM (PEPIP) and HOSPITAL ALL RISK PROPERTY PROGRAM (HARPP) as their respective rights and interests may appear which now exist or which hereafter may be created or acquired and which are owned, financially controlled or actively managed by the herein named interest, all jointly, severally or in any combination of their interests, for account of whom it may concern (all hereinafter referred to as Member(s) / Entity(ies).

DECLARATION: Various Declarations as on file with Insurer

POLICY PERIOD: July 1, 2024 to July 1, 2025

TERRITORY: WORLD-WIDE

RETROACTIVE DATE:

APIP/PEPIP

For new members – the retro active date will be the date of addition

July 1, 2023 For existing members included on the July 1, 2023/24 policy

July 1, 2022 For existing members included on the July 1, 2022/23 policy

July 1, 2021 For existing members included on the July 1, 2021/22 policy

July 1, 2020 For existing members included on the July 1, 2020/21 policy

July 1, 2019 For existing members included on the July 1, 2019/20 policy

July 1, 2018 For existing members included on the July 1, 2018/19 policy

July 1, 2017 For existing members included on the July 1, 2017/18 policy

July 1, 2016 For existing members included on the July 1, 2016/17 policy

July 1, 2015 For existing members included on the July 1, 2015/16 policy

July 1, 2014 For existing members included on the July 1, 2014/15 policy

July 1, 2013 For existing members included on the July 1, 2013/14 policy

July 1, 2012 For existing members included on the July 1, 2012/13 policy

July 1, 2011 For existing members included on the July 1, 2011/12 policy

July 1, 2010 For existing members included on the July 1, 2010/11 polic y

July 1, 2010 For existing insured's included on the July 1, 2010/11 policy

CSU

July 1, 2008 California State University and CSU Auxiliary Organizations

INSURER:				Lloyd's of London - Beazley Syndicate: Syndicates 2623 - 623 - 100% Liberty Surplus Insurance Corporation (Ironshore) Associated Industries Insurance Company, Inc. (AmTrust Financial)
COVERAGES & LIMITS:	**Ai.**	$	55,000,000	**Annual Policy and Program Aggregate Limit of Liability** (subject to policy exclusions) for all Insureds/Members combined (Aggregate for all coverages combined, including Claims Expenses), subject to the following limits and sub-limits as noted.
	Aii.	$	2,000,000	**Insured/Member Annual Aggregate Limit of Liability** (subject to policy exclusions) for each Insured/Member, **within** the Annual Policy and Program Aggregate Limit of Liability **and** JPA/Pool Annnual Aggregate Limit of Liability (Aggregate for all coverages combined, including Claim Expenses) subject to the following limits and sub-limits as noted.
BREACH RESPONSE				
Breach Response Costs:		$	500,000	**Aggregate Limit of Liability** for each Insured/Member (Limit is increased to $1,000,000 if Beazley Nominated Services Providers are used)
FIRST PARTY LOSS				
Business Interruption and Dependent Business Interruption Aggregate Sub-Limit:		$	750,000	**Aggregate Limit of Liability** for each Insured/Member
Business Interruption Loss Resulting from Security Breach		$	750,000	**Aggregate Limit of Liability** for each Insured/Member (Within the $750,000 Business Interruption and Dependent Business Interruption Aggregate Sublimit)
Business Interruption Loss Resulting from System Failure:		$	500,000	**Aggregate Limit of Liability** for each Insured/Member (Within the $750,000 Business Interruption and Dependent Business Interruption Aggregate Sublimit)

Dependent Business Loss Resulting from Security Breach:	$	750,000	**Aggregate Limit of Liability** for each Insured/Member (Within the $750,000 Business Interruption and Dependent Business Interruption Aggregate Sublimit)
Dependent Business Loss Resulting from System Failure:	$	100,000	**Aggregate Limit of Liability** for each Insured/Member (Within the $750,000 Business Interruption and Dependent Business Interruption Aggregate Sublimit)
Cyber Extortion Loss:	$	750,000	**Aggregate Limit of Liability** for each Insured/Member
Data Recovery Costs:	$	750,000	**Aggregate Limit of Liability** for each Insured/Member
Data & Network Liability:	$	2,000,000	**Aggregate Limit of Liability** for each Insured/Member for all Damages and Claims Expenses
Regulatory Defense & Penalties:	$	2,000,000	**Aggregate Limit of Liability** for each Insured/Member
Payment Card Liabilities & Costs:	$	2,000,000	**Aggregate Limit of Liability** for each Insured/Member
Media Liability:	$	2,000,000	**Aggregate Limit of Liability** for each Insured/Member for all Damages and Claims Expenses
eCRIME			
Fraudulent Instruction:	$	75,000	**Aggregate Limit of Liability** for each Insured/Member
Funds Transfer Fraud:	$	75,000	**Aggregate Limit of Liability** for each Insured/Member
Telephone Fraud:	$	75,000	**Aggregate Limit of Liability** for each Insured/Member
CRIMINAL REWARD			
Criminal Reward:	$	25,000	**Aggregate Limit of Liability** for each Insured/Member
COVERAGE ENDORSEMENT(S)			
Reputation Loss:	$	200,000	**Aggregate Limit of Liability** for each Insured/Member
Claims Preparation Costs for Reputation Loss Claims Only:	$	50,000	**Aggregate Limit of Liability** for each Insured/Member

Computer Hardware Replacement Costs:	$	200,000	**Aggregate Limit of Liability** for each Insured/Member
Invoice Manipulation:	$	100,000	**Aggregate Limit of Liability** for each Insured/Member
Cryptojacking:	$	50,000	**Aggregate Limit of Liability** for each Insured/Member

RETENTION:	$	TBD	CSU Auxiliary Organizations only
	$	50,000	Per Claim for each Member/Insured with Total Insured Value (TIV) up to $250,000,000 at the time of policy inception
		8	Hour waiting period for Dependent/Business Interruption Loss
	$	100,000	Per Claim for each Member/Insured with Total Insured Value (TIV) greater than $250,000,000 and up to $750,000,000 at the time of policy inception
		8	Hour waiting period for Dependent/Business Interruption Loss
	$	250,000	Per Claim for each Member/Insured with Total Insured Value (TIV) greater than $750,000,000 at the time of policy inception
		8	Hour waiting period for Dependent/Business Interruption Loss

NOTICES:

Policy coverage of this policy provides coverage on a claims made and reported basis; except as otherwise provided, coverage under noted coverage schedule applies only to claims first made against the Insured/Member and reported to underwriters during the policy period. Claims expenses shall reduce the applicable limit of liability and are subject to the applicable retention.

This is a shared limit policy among the Named Insureds. The per Insured/Member policy limits are on a per claim or incident for each Insured/Member basis, sub-limits listed are aggregated per Insured/Member and are within the total Insured/Member aggregate limit. In the event of a claim/incident with multiple Insureds/Members exhausting the program aggregate limit provided by the Insurer to Insureds/Members, payment to all Insureds/Members for the claim/incident will be determined by the Insurer. Where coverages are aggregated, sub-limit and limits apply to all Insureds/Members for the entire Policy Period unless specifically stated otherwise. The policy aggregate limit is not a per Insured/Member maximum limit.

EXTENDED REPORTING PERIOD:

For Named Insured - To be determined at the time of election (additional premium will apply)

SPECIFIC COVERAGE PROVISIONS:

A. **Breach Response** indemnifies the Insured/Member for Breach Response Costs incurred by the Insured/Member because of an actual or reasonably suspected Data Breach or Security Breach that the Insured first discovers during the Policy Period.

B. **First Party Loss**

Business Interruption Loss indemnifies the Insured/Member for a Business Interruption Loss sustained as a result of a Security Breach or System Failure that the Insured first discovers during the Policy Period.

Dependent Business Interruption Loss indemnifies the Insured/Member for a Dependent Business Interruption Loss sustained as a result of a Security Breach or a System Failure that the Insured first discover during the Policy Period.

Cyber Extortion Loss indemnifies the Insured/Member for a Cyber Extortion Loss incurred as a result of an Extortion Threat first made against the Insured/Member during the Policy Period.

Data Recovery Costs indemnifies the Insured/Member for Data Recovery Costs incurred as a direct result of a Security Breach or System Failure that the Insured first discovers during the Policy Period.

C. **Liability**

Data & Network Liability pays Damages and Claims Expenses, which the Insured is legally obligated to pay because of any Claim first made against any Insured during the Policy Period for a Data Breach, a Security Breach, the Insured's failure to disclose a Data Breach or Security Breach, or failure of the Insured to comply with the part of a Privacy Policy that specifically is related to disclosure, access or procedures related to Personally Identifiable Information.

Regulatory Defense & Penalties pays Penalties and Claims Expenses, which the Insured is legally obligated to pay because of a Regulatory Proceeding first made against any Insured during the Policy Period for a Data Breach or a Security Breach.

Payment Card Liabilities & Costs indemnifies the Insured/Member for PCI Fines, Expenses and Costs which it is legally obligated to pay because of a Claim first made against any Insured during the Policy Period.

Media Liability pays Damages and Claims Expenses, which the Insured is legally obligated to pay because of any Claim first made against any Insured during the Policy Period for electronic Media Liability.

D. **eCrime** indemnifies the Insured/Member for any direct financial loss sustained resulting from:

- *Fraudulent Instruction*
- *Funds Transfer Fraud*
- *Telephone Fraud*

That the Insured first discovers during the Policy Period.

E. **Criminal Reward** indemnifies the Insured/Member for Criminal Reward Funds.

Coverage Endorsement(s)	**Reputational Loss** indemnifies the Insured Organization for Reputation Loss that the Insured Organization sustains solely as a result of an Adverse Media Event that occurs during the Policy Period, concerning: a Data Breach, Security Breach, or Extortion Threat that the Insured first discovers during the Policy Period **Computer Hardware Replacement Costs** is part of the Extra Expense coverage. Extra Expense means reasonable and necessary expenses incurred by the Insured Organization during the Period of Restoration to minimize, reduce or avoid Income Loss, over and above those expenses the Insured Organization would have incurred had no Security Breach, System Failure, Dependent Security Breach or Dependent System Failure occurred; and includes reasonable and necessary expenses incurred by the Insured Organization to replace computers or any associated devices or equipment operated by, and either owned by or leased to, the Insured Organization that are unable to function as intended due to corruption or destruction of software or firmware directly resulting from a Security Breach **Invoice Manipulation** indemnifies the Insured Organization for Direct Net Loss resulting directly from the Insured Organization's inability to collect Payment for any goods, products or services after such goods, products or services have been transferred to a third party, as a result of Invoice Manipulation that the Insured first discovers during the Policy Period. Invoice Manipulation means the release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a Security Breach or a Data Breach. **Cryptojacking** indemnifies the Insured Organization for any direct financial loss sustained resulting from Cryptojacking that the Insured first discovers during the Policy Period. Cryptojacking means the Unauthorized Access or Use of Computer Systems to mine for Digital Currency that directly results in additional costs incurred by the Insured Organization for electricity, natural gas, oil, or internet.

EXCLUSIONS:
(Including but not limited to)

Coverage does not apply to any claim or loss from:

- Bodily Injury or Property Damage
- Trade Practices and Antitrust
- Gathering or Distribution of Information
- Prior Known Acts & Prior Noticed Claims
- Racketeering, Benefit Plans, Employment Liability & Discrimination
- Sale or Ownership of Securities & Violation of Securities Laws
- Criminal, Intentional of Fraudulent Acts
- Patent, Software Copyright, Misappropriation of Information
- Governmental Actions
- Other Insureds & Related Enterprises
- Trading Losses, Loss of Money & Discounts
- Media-Related Exposures – Contractual liability or obligation
- Nuclear Incident
- Radioactive Contamination
- Sanctions Limitation
- War and Civil War
- Asbestos, Pollution and Contamination
- First Party Loss – with respects: 1. seizure, nationalization, confiscation, or destruction of property or data by order of any governmental or public authority; 2. costs or expenses incurred by the Insured to identify or remediate software program errors or vulnerabilities or update, replace, restore, assemble, reproduce, recollect or enhance data or Computer Systems to a level beyond that which existed prior to a Security Breach, System Failure, Dependent Security Breach, Dependent System Failure or Extortion Threat; 3. failure or malfunction of satellites or of power, utility, mechanical or telecommunications (including internet) infrastructure or services that are not under the Insured Organization's direct operational control; or 4. fire, flood, earthquake, volcanic eruption, explosion, lightning, wind, hail, tidal wave, landslide, act of God or other physical event.
- Website Tracking Exclusion specific to hospitals as defined by: A health facility with overall administrative and professional responsibility and an organized medical staff that provides 24-hour inpatient care, including the following services: medical, nursing, surgical, anesthesia, laboratory, pharmacy, and dietary services.

NOTICE OF CLAIM:	• IMMEDIATE NOTICE must be made to Beazley NY of all potential claims and circumstances (assistance, and cooperation clause applies) • Claim notification under this policy is to: Beazley Group Attn: TMB Claims Group 45 Rockefeller Plaza, 16th Floor New York, NY 10111 bbr.claims@beazley.com

NOTICE OF CANCELLATION:	10 days for non-payment of premium
OTHER SERVICES	Unlimited Access to Beazley Breach Solutions website
BROKER:	ALLIANT INSURANCE SERVICES, INC. License No. 0C36861

NOTES:

- ***Some coverage, limits, sub-limits, terms and conditions will change, as negotiations are ongoing. Changes will be documented and accompany the Binder Confirmation for July 1, 2024 bound terms. Coverage outlined in this Proposal is subject to the terms and conditions being negotiated with the policy. To be finalized and presented at Program Inception.***
- ***Please refer to Policy for specific terms, conditions and exclusions***
- ***Change in Total Insurable Values will result in adjustment in premium***

SUMMARY OF CYBER INSURANCE CHANGES

THE FOLLOWING ITEMS ARE BOUND CHANGES FOR THE 2024-2025 POLICY TERM

Coverage	2023-2024	2024-2025 Proposed Changes
Beazley Breach Response Endorsement	Coverage offered to new and existing Members – Underwriting required	Coverage offered to new and existing Members – Underwriting required
Retention Buy Down	Coverage is being offered to new and existing members; underwriting required	Coverage is being offered to new and existing members; underwriting required
New members to APIP Cyber Core-Mid Term Transactions	New this year; no underwriting, all members requesting core coverage are eligible. Ransomware application, statement of no losses, and AFB warranty required.	No underwriting, all members requesting core coverage are eligible. Ransomware application, statement of no losses, and AFB warranty required.
Beazley Core Coverage-Website Tracking Exclusion	Not included	Website Pixel Tracking Exclusion specific to Hospitals defined as a Health Facility with overall administrative and professional responsibility and organized medical staff that provides 24-hour inpatient care, including the following services: Medical, nursing, surgical, anesthesia, laboratory, pharmacy, and dietary services.
Beazley Core Coverage-New Boost offering	Not Included	By endorsement and included only with the BBR purchase. Open to all members. Provides full limit coverage for some First Party Limits; Business Interruption, Cyber Extortion, and Data Recovery.
Beazley Core Coverage- increased sublimit	Computer Hardware $100,000 Reputational Loss $100,000 Cryptojacking $25,000	Increased Computer Hardware Replacement to $200,000. Increased Reputational Loss Coverage to $200,000 Increased Cryptojacking to $50,000
APIP Program Aggregate Change	Program Aggregate $45,000,000	Increased this year to $55,000,000