

APIP Cyber Coverage Overview

The APIP Cyber Program general coverages and terms are summarized below. The following information is meant to be an overview, for more detail, please consult your client team and the policy language.

Limit/Retention Description	Limit/Retention Amount (2019/20)	Limit/Retention Amount (2020/21)
Program Aggregate Limit	\$25,000,000	\$25,000,000
Per Member Aggregate Limit	\$2,000,000	\$2,000,000
Retention	\$50,000*/\$100,000*/8 hours	\$50,000*/\$100,000*/8 hours
Breach Response	\$500,000 (Non- Beazley vendor) / \$1,000,000 (Beazley Vendor)	\$500,000 (Non- Beazley vendor) / \$1,000,000 (Beazley Vendor)
Business Interruption Resulting from Security Breach	\$2,000,000	\$2,000,000
Business Interruption Resulting from System Failure	\$500,000	\$500,000
Dependent Business Loss Resulting from Dependent Security Breach	\$750,000	\$750,000
Dependent Business Loss Resulting from Dependent System Failure	\$100,000	\$100,000
Cyber Extortion Loss	\$2,000,000	\$2,000,000
Data Recovery Costs	\$2,000,000	\$2,000,000
Data & Network Liability	\$2,000,000	\$2,000,000
Regulatory Defense & Penalties	\$2,000,000	\$2,000,000
Payment Card Liabilities & Costs	\$2,000,000	\$2,000,000
Media Liability	\$2,000,000	\$2,000,000
Fraudulent Instruction	\$75,000	\$75,000
Funds Transfer Fraud	\$75,000	\$75,000
Telephone Fraud	\$75,000	\$75,000
Criminal Reward	\$25,000	\$25,000
Reputation Loss	\$50,000	\$50,000
Claims Preparation Costs for Reputation Loss Only Claims	N/A	\$50,000
Computer Hardware Replacement	\$75,000	\$75,000
Invoice Manipulation	\$100,000	\$100,000
Cryptojacking	N/A	\$25,000

* Retention is based on if TIVs are below or above \$500M.

**Blue font denotes changes from the 2019/20 policy to the 2020/21 policy

APIP Cyber Coverage Overview

- **Breach Response**
 - Legal advice from attorney
 - Computer security expert
 - PCI forensics investigator
 - Notification
 - Call center
 - Credit monitoring
 - Public relations and crisis management
- **Business Interruption Resulting from Security Breach**
 - Income loss
 - Forensic expenses
 - Extra expenses
 - Does not include unfavorable business conditions, loss of market or any consequential loss
- **Business Interruption Resulting from System Failure**
 - Income loss
 - Forensic expenses
 - Extra expenses
 - Does not include unfavorable business conditions, loss of market or any consequential loss
- **Dependent Business Loss Resulting from Dependent Security Breach**
 - Income loss
 - Forensic expenses
 - Extra expenses
 - Does not include unfavorable business conditions, loss of market or any consequential loss
- **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
- **Cyber Extortion Loss**
 - Money, digital currency, marketable goods or services demanded to prevent or terminate an extortion threat

APIP Cyber Coverage Overview

- **Data Recovery Costs**
 - Reasonable and necessary expenses to regain access to, replace or restore data
- **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
- **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

APIP Cyber Coverage Overview

- **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
 - **Claims Preparation Costs** means reasonable and necessary costs that the Named Insured incurs to contract with a third party to prepare a proof of loss demonstrating Reputational Loss.
- **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
- **General Data Protection Regulation Endorsement**
 - Coverage for non-compliance with the following EU GDPR Articles: 5.1(f), 32, 33, & 34