IRMA Cyber Suite Coverage Summary

CYBER SUITE COVERAGE
SUPPLEMENTAL DECLARATIONS
November 1, 2019 to November 1, 2020

Annual Aggregate Limit per Member:	**$1,000,000**
Deductible Per Occurrence:	**$ 10,000**
DATA COMPROMISE RESPONSE EXPENSES	**Included in $1M limit**
Sublimits Per Occurrence	
Forensic IT Review:	$500,000
Legal Review:	$500,000
Public Relations:	$5,000
Regulatory Fines and Penalties:	$500,000
PCI Fines and Penalties:	$500,000
COMPUTER ATTACK	**Included in $1M limit**
Sublimits Per Occurrence	
Loss of Business:	$500,000
Public Relations:	$5,000
CYBER EXTORTION	**Included in $1M limit**
Sublimit Per Occurrence:	$100,000**
MISDIRECTED PAYMENT FRAUD	**Included in $1M limit**
Sublimit Per Occurrence:	$25,000
COMPUTER FRAUD	**Included in $1M limit**
Sublimit Per Occurrence:	$25,000
DATA COMPROMISE LIABILITY	**Included in $1M limit**
NETWORK SECURITY LIABILITY	**Included in $1M limit**
ELECTRONIC MEDIA LIABILITY	**Included in $1M limit**

**IRMA provides excess cyber extortion coverage of $75,000 over the HSB sublimit of $25,000.
**IRMA provides additional $100,000 limits in 1st Party Property coverage.

DESCRIPTION OF CYBER SUITE COVERAGES

Coverage 1 - Data Compromise Response Expenses

Data Compromise coverage is triggered by the Member's discovery that personal information in the Member's care, custody or control or from third parties with whom the Member has a direct relationship and to whom the Member has entrusted the personal data has been lost, stolen or inadvertently published. This also includes breaches of data that is sensitive and personal to individuals, whether it can be used to commit fraud, where notification is required by law.

The covered breach may be:

- Electronic (theft of electronic files)
- Physical (theft of hardcopy files)
- Procedural (mistakenly posting personal information to a website or printing Social Security Numbers on mailing labels)
- Fraud-related (such as the purchase of information by sham companies)

Forensic Information Technology
If the breach involves electronic hacking, it may be necessary to hire outside computer experts to determine the nature and extent of the breach.

Legal Review
We provide coverage should a company dealing with a potential breach of personal data desire to consult with legal counsel. The legal review coverage is intended to make sure that Members have the access and means to obtain professional legal advice.

Notification to Affected Individuals
Notification to Affected Individuals provides for reimbursement of expenses associated with the notification of "affected individuals" – that is to say, those whose personal information was compromised. Often this may include a package of materials mailed to the "affected individuals".

Services to Affected Individuals
Services to Affected Individuals provides coverage for the following services to "affected individuals":

- Packet of informational materials
- Toll-free help line

- One year of credit monitoring
- Identity Recovery case management

Public Relations Services
Public Relations Services allows for a professional public relations firm to review and respond to the potential impact of the data compromise event on the Member's business relationships.

It includes costs to implement public relations recommendations of a professional public relations firm. This may include advertising and special promotions designed to retain the relationship with affected individuals. However, the following promotions are not covered:

- Provided to any of your directors or employees; or
- Costing more than $25 per "affected individual".

The coverage is triggered by the notifications of "affected individuals".

Regulatory Fines and Penalties
Any fine or penalty imposed, to the extent such fine or penalty is legally insurable under the law of the applicable jurisdiction.

PCI Fines and Penalties
Any Payment Card Industry fine or penalty imposed under a contract to which you are a party. PCI Fines and Penalties do not include any fraudulent charges, assessments or increased transaction costs.

Coverage 2 – Computer Attack

The Computer Attack coverage is triggered by the Member's discovery that a computer attack has affected a computer system owned or leased by the Member and under the Member's control, or is a computer system that is operated by a third party service provider used for the purpose of providing hosted computer application services to you or for processing, maintaining, hosting or storing your electronic data, pursuant to a written contract with you for such services. However, such computer or other electronic hardware operated by such third party shall only be a "computer system" with respect to the specific services provided by such third party to you under such contract.

A computer attack may be:

- A hacking event or other instance of an unauthorized person gaining access to the computer system
- An attack against the system by a virus or other malware
- A denial of service attack against the Member's system

Data Restoration Costs
Coverage for the cost of a professional firm hired by the Member to replace lost or corrupted data

from electronic sources.

Data Recreation Costs
Coverage for the cost of a professional firm hired by the Member to research, recreate and replace lost or corrupted data from *non*-electronic sources.

System Restoration Costs
Coverage for the cost of a professional firm hired by the Member to restore its computer system to its pre-attack level of functionality by replacing or reinstalling software, removing malicious code and correcting the configuration of the Member's computer system.

Loss of Business
Coverage for business income lost by the Member and extra expenses incurred by the Member during the period when system and data recovery activities are taking place.

Extended Income Recovery
Extended income recovery would provide the coverage for the component of the business income that had still not recovered to historical levels after the period of recovery has completed.

Public Relations Services
Coverage for assistance from a professional public relations firm in communicating with outside parties concerning the Computer Attack and the Member's response.

Coverage 3 – Cyber Extortion

The Cyber Extortion coverage is triggered by the Member's receipt of a cyber extortion threat. Coverage for responding to extortion threats which include:

- The cost of a negotiator or investigator retained by you in connection with a cyber extortion threat
- Any amount paid by you in response to a credible cyber extortion threat to the party that made the cyber extortion threat for the purposes of eliminating the threat.

Coverage 4 - Misdirected Payment Fraud

The Coverage is triggered when the Member is the victim of a wrongful transfer event - an intentional and criminal deception of the Member or a financial institution with which the Member has an account. The deception must be perpetrated by a person who is not an employee, using email, facsimile or telephone communications to induce the Member or the financial institution to send money or divert a payment. The deception must result in direct financial loss to a Member. Once Triggered, the coverage provides reimbursement for the amount fraudulently obtained from the Member.

Coverage 5 - Computer Fraud

The Computer Fraud coverage is triggered when the Member is the victim of a computer fraud event - unauthorized access to the Member's computer system that leads to the intentional, unauthorized and fraudulent entry of or change to data or instructions within the computer system. Such fraudulent entry or change must be conducted by a person who is not an employee, executive or independent contractor. Such fraudulent entry or change must cause money to be sent or diverted. The fraudulent entry or change must result in direct financial loss to the Member. Once triggered, the coverage provides reimbursement for the amount fraudulently obtained from the Member.

Coverage 6 - Data Compromise Liability

Data Compromise Liability Coverage is designed as a complement to the Response Expense (first party) Data Compromise Coverage. Before there can be a loss under Liability, there must first be a covered loss under the Response Expenses (first party) Data Compromise Coverage. If one or more such "affected individuals", or a government entity on behalf of such individuals, sue the Member, then coverage is provided for defense and settlement costs, subject to the coverage limit.

Coverage 7 - Network Security Liability

Network Security Liability Coverage is triggered by the Member's receipt of notice of a network security liability suit. The network security liability suit can be a civil action, an alternate dispute resolution proceeding or a written demand for money. The network security liability suit must be initiated by a third party who alleges that a systems security failure on the part of the Member allowed one or more of the following to happen:

- The breach of third-party business information
- The unintended propagation or forwarding of malware
- The unintended abetting of a denial of service attack

Network Security Liability coverage provides for defense costs (within the coverage limit) and associated settlement and judgment costs arising from an action brought by third parties who allege certain injuries as a result of a failure in the Member's systems security.

Coverage 8 - Electronic Media Liability

Electronic Media Liability Coverage is triggered by the Member's receipt of notice of an electronic media liability suit. The electronic media liability suit can be a civil action, an alternate dispute resolution proceeding or a written demand for money. The electronic liability suit must be initiated by a third party who alleges that the display of information in electronic form by the Member on a website resulted in:

- The infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark or service name;

- Defamation against a person or organization that is unintended; or
- A violation of a person's right of privacy, including false light and public disclosure of private facts.

Risk Management Resources

eRisk Hub

By purchasing the HSB Cyber Suite coverage IRMA is given access to a risk management portal referenced as eRisk Hub. The eRisk Hub website can be found at:

https://irmarisk.org/Risk-Management/Cyber-Risk-E-Hub.aspx

Key features of the portal include:

- Incident Response Plan Roadmap – suggested steps business can take following a data breach incident. Having an incident response plan prepared in advance of a breach can be useful for defense of potential litigation.
- Online Training Modules – ready-to-use training for business owners on privacy best practices and Red Flag Rules.
- Risk Management Tools – assist business in managing their data breach and other cyber exposures including self-assessments and state breach notification laws.
- eRisk Resources – a directory to quickly find external resources on pre- and post-breach disciplines, computer attack response and data recovery.
- News Center – cyber risk stories, security and compliance blogs, security news, risk management events, and helpful industry links.
- Learning Center – best practices and white papers written by leading authorities.