MIDWEST PUBLIC RISK

In the Event of a

Cyber Incident or Claim

What you should know about a Cyber Security Incident

A cyberattack is a deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Cyberattacks may include the following:

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spoofing, spyware, Trojans and viruses
- Denial-of-service and distributed denial-of-service attacks
- Breach of access, System infiltration, Website defacement
- Password sniffing, Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

Responding to a Cyber Security Incident

1. Report the claim to Beazley: email ***bbr.claims@beazley.com*** and follow up with a call: 1-866-567-8570. Include the following information in the email.
    a. Name of your organization
    b. Policy number **PH1504944**, mention you are a member of Midwest Public Risk
    c. Description of the event
    d. Timeline of incident
    e. Does the problem take place on a server or a workstation?
    f. How you discovered the issue
    g. Provide a contact name and details

Questions? Contact Director of Insurance and Risk
Melanie Matt at Melanie@MPRisk.org or at 816-292-7541.

What to expect from Beazley

1. The Beazley Breach Response team will reach out to the contact person within one business day to schedule a phone call to discuss the incident.
2. They will assist with any necessary investigation and response services.
3. Beazley will provide guidance throughout the investigation and response process.

MPR Coverage Limits

COVERAGES & LIMITS:

$	2,000,000	Information Security & Privacy Liability.
$	500,000	Privacy Notification Costs. Limit is $1,000,000 if Beazley vendor services are used.
$	2,000,000	Claims Expenses and Penalties for Regulatory Defense and Penalties PCI Fines and Penalties limit of $100,000.
$	2,000,000	First Party Business Interruption Sub-Limits of Liability
$	50,000	1) Hourly Sublimit
$	50,000	2) Forensic Expense Sublimit
$	150,000	3) Dependent Business Interruption Sublimit.

Questions? Contact Director of Insurance and Risk
Melanie Matt at Melanie@MPRisk.org or at 816-292-7541.

SPECIFIC COVERAGE PROVISIONS:

A. Information Security and Privacy Liability pays on behalf of the Member damages and claims expenses excess of the retention which the Member shall become legally obligated to pay because of any claim, including a claim for violation of a privacy law first made against the Member and reported to underwriters during the policy period for

- theft, loss or unauthorized disclosure of personally identifiable non-public information or third party corporate information that is in the care, custody or control of the Member, or an independent contractor that is holding, processing or transferring such information on behalf of the Member.
- Acts or incidents that directly result from the failure of computer security to prevent a security breach including:
    - o Alteration, corruption, destruction, deletion, or damage to a data asset stored on computer systems
    - o Failure to prevent transmission of malicious code from computer systems to third party computer systems
    - o Participation in a denial of service attack directed against a third party computer system
- The failure to timely disclose any of the above in violation of any breach notice law
- The failure to comply with a privacy policy involving the disclosure, sharing or selling of personally identifiable non-public information
- The failure to administer an identity theft prevention program

B. Privacy Notification Costs pay the Member for reasonable and necessary costs to comply with a breach notice law

EXCLUSIONS (Including, but not limited to):

Coverage does not apply to any claim or loss from

- Bodily Injury or Property Damage
- Any employer-employee relations, policies, practices
- Contractual Liability or Obligation
- Any actual or alleged act, error or omission or breach of duty by any director, officer, manager if claim is brought by principals, officers, directors, stockholders and the like
- Anti-Trust violations
- Unfair trade practices
- Unlawful collection or acquisition of Personally Identifiable Non-Public Information
- Distribution of unsolicited e-mails, facsimile, audio or video recording
- Prior knowledge or previously reported incidents
- Incidents occurring prior to retroactive date/continuity date
- Any act, error, omission, of computer security if occurred prior to policy inception
- Collusion
- Securities Act Violations
- Fair Labor Act Violations
- Discrimination
- Intentional Acts with regard to Privacy and Security Breach
- Infringement - Patent and Copyright
- Federal Trade Commission and related state, federal, local and foreign governmental activities
- Insured vs. Insured
- Money/Securities/Funds Transfer
- Broadcasting, Publications and Advertising
- War and Terrorism
- Pollution
- Nuclear Incident
- Radioactive Contamination