UW

# Cyber Enhancement Endorsement: Understanding Your Coverage

**Since 2014, Community Insurance Corporation has provided cyber liability insurance through our Cyber Enhancement Endorsement – included at no additional premium. Cyber liability insurance provides coverage for many expenses that may arise from a data breach involving personal information or a security incident resulting in unauthorized access or misuse of your computer systems. Just as cyber, privacy and regulatory risks are evolving, so are our cyber insurance coverages. CIC continues its aim to deliver responsive coverage to address these emerging risks and trends affecting our members: emerging threat vectors, soon-to-be-enforced privacy regulations, and different risks that are developing because of new technologies.**

**This document provides an overview of the updated coverage in our Cyber Enhancement Endorsement and our assistive approach to improving your cybersecurity efforts across your organization. This document is intended to provide an overview summary of the coverage – refer to the terms and conditions of the actual coverage form.**

## What coverage forms and limits are included in your endorsement?

At Community Insurance Corporation (CIC), we provide more than data breach coverage response costs. We have considered our members' risk profiles to include and provide added coverage parts for a range of information security and online risks, including:

| | |
|---|---|
| FIRST PARTY LOSS | **Business Interruption Loss:** Coverage is provided for loss of revenue due to an actual interruption of your business operations caused by a security incident. |
| | **Cyber Extortion Loss**: Coverage is provided for loss resulting from an extortion threat to perpetuate the unauthorized access or use of your computer systems, prevent access to your computer systems or data, or steal, misuse, or publicly disclose data, PII, or third-party information. Extortion payments include money, digital currency, marketable goods, or services. |
| | **Data Recovery Costs:** Coverage to provide forensic and other costs to regain access to, replace, or restore data. |
| | **Reputation Loss:** Coverage is provided for income loss that results from reputation damage following a data breach or security incident. |
| LIABILITY | **Data & Network Liability:** Coverage is provided for damages and claim expense you are legally obligated to pay as a result of a claim from a data breach or security incident. In other words, coverage to pay court costs, investigation fees, monetary judgment, award, or settlement assessed to your district through legal proceedings for involvement in a data breach or security incident claim. |
| | **Regulatory Defense & Costs:** Coverage is provided to pay civil fines and penalties assessed to your entity by a regulatory authority relating to a data breach or security incident. |
| | **Payment Card Liabilities & Costs:** Coverage is provided for any PCI fines owed by you under the terms of a merchant services agreement. Coverage is also provided for a PCI Forensic Investigator to investigate a data breach involving payment card data and for a Qualified Security Assessor to certify and assist in attesting to your PCI compliance. |
| | **Media Liability:** This coverage protects your entity from acts, errors, and omissions in the course of disseminating or releasing media material (i.e., words, numbers, images, or graphics) to the public. |

| | |
|---|---|
| E-CRIME | **Fraudulent Instruction:** This coverage protects your entity from loss resulting from the transfer, payment or delivery of money or securities as a result of fraudulent instructions provided by a third party that is intended to mislead you (e.g., social engineering techniques). |
| | **Funds Transfer Fraud:** Coverage is provided for the loss resulting from fraudulent instructions by a third party issued to a financial institution directing such institution to transfer, pay or deliver money from your account(s). |
| | **Telephone Fraud:** This coverage protects your organization from loss resulting from a third-party gaining access to and using your organization's telephone system in an unauthorized manner. |
| | **Criminal Reward:** Any amount offered or paid by your organization with our prior written consent for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to your coverages. |

## When does your policy respond?

While the response of each coverage will depend upon the specific terms of each coverage part, a number of coverages generally respond in relation to an actual or reasonably suspected data breach or security incident.

## What potential insurable response costs are included?

Regardless of the source of the claim, the costs associated with a cyber incident can be high. Response costs may include:

- Hiring counsel to advise on notification and other legal requirements.
- Hiring forensic experts to investigate the incident or recreate the data.
- Notifying potentially affected persons that their information was compromised.
- Setting up a call center to respond to inquiries.
- Providing credit monitoring, identity monitoring or other solutions.
- Retaining public relations professionals or crisis managers.
- Compensation for lost income resulting from the incident.
- Costs incurred to recover data.
- Regulatory costs, fines, and punitive damages.
- Litigation defense costs and damages.

## Reporting and responding to a security breach or incident

**If you suspect your organization has been a victim of a cybersecurity incident or data breach, one of your first actions should be to notify us as soon as possible**. This will help ensure that you are not jeopardizing coverage for any costs associated with the incident. If there is a covered data breach or security incident, we will guide you throughout the entire process. If we determine that assigning external support is appropriate, we will select providers chosen by us, from our panel, in consultation with you.

**As soon as possible following a security breach or incident activity, please contact**:

**Sheila Mishich, AIC**
Litigation Case Manager
800.236.6885
sheila.mishich@charlestaylor.com

**PLEASE DO NOT HIRE OR RETAIN YOUR OWN VENDOR(S) TO INVESTIGATE SUSPECTED OR ACTUAL CYBERCRIMINAL ACTIVITY. PLEASE CONTACT COMMUNITY INSURANCE CORPORATION AS SOON AS POSSIBLE.**

**Important Tips:**

- Restrict communications and use caution when discussing the incident. Limit discussions to a need-to-know basis, with communications taking place over the phone or face-to-face rather than email. And avoid using the term "breach" which can trigger legal obligations. Instead, call the event a "security incident" or simply state what it is (e.g., a lost laptop).
- Do not turn off or reboot any systems. Record critical facts regarding the incident (date and time, when the incident was discovered, who discovered the incident, what occurred, what systems and information were potentially compromised).
- Secure the scene to preserve evidence. Do not allow anyone to take any action on affected systems.

## What cybersecurity resources and services are available?

Cybersecurity is one of the most important issues facing our members and the public today. Depending on your organization's structure, protecting data and other information technology (IT) assets from loss, destruction, or unauthorized access is your responsibility, but you don't have to do this alone. CIC can play an important role in helping you protect your organization from cyberattacks, data breaches, and other cyber incidents. Contact us and we can work towards proactive steps that you can take to minimize risks and get prepared before a cyberattack, data breach, or other cyber incident happens.

**Seth Johnson**
Cyber Risk Management Consultant
715.614.4150
seth.johnson@charlestaylor.com

## Have more questions? Need consultation?

| Coverage | Cyber Risk Management & Services |
|---|---|
| **Paul Schwegel** | **Seth Johnson** |
| **Director of Underwriting Programs** | **Cyber Risk Management Consultant** |
| **P**: 262.252.6556 | **P**: 715.614.4150 |
| **E**: paul.schwegel@charlestaylor.com | **E**: seth.johnson@charlestaylor.com |

| Coverage & Limit Structure | |
|---|---|
| **First Party Loss** | **Limit** |
| **Business Interruption Loss**: Coverage is provided for loss of revenue due to an actual interruption of your business operations caused by a security incident. | 500,000 |
| **Cyber Extortion Loss**: Coverage is provided for loss resulting from an extortion threat to perpetuate the unauthorized access or use of your computer systems, prevent access to your computer systems or data, or steal, misuse, or publicly disclose data, PII, or third-party information. Extortion payments include money, digital currency, marketable goods, or services. | 500,000 |
| **Data Recovery Cost**s: Coverage to provide forensic and other costs to regain access to, replace, or restore data. | 500,000 |
| **Reputation Loss**: Coverage is provided for income loss that results from reputation damage following a data breach or security incident. | 500,000 |
| **Liability** | |
| **Data & Network Liability**: Coverage is provided for damages and claim expense you are legally obligated to pay as a result of a claim from a data breach or security incident. In other words, coverage to pay court costs, investigation fees, monetary judgment, award, or settlement assessed to your district through legal proceedings for involvement in a data breach or security incident claim. | 1,000,000 |
| **Regulatory Defense & Costs**: Coverage is provided to pay civil fines and penalties assessed to your entity by a regulatory authority relating to a data breach or security incident. | 50,000 |
| **Payment Card Liabilities & Costs**: Coverage is provided for any PCI fines owed by you under the terms of a merchant services agreement. Coverage is also provided for a PCI Forensic Investigator to investigate a data breach involving payment card data and for a Qualified Security Assessor to certify and assist in attesting to your PCI compliance. | 50,000 |
| **Media Liability**: This coverage protects your entity from acts, errors, and omissions in the course of disseminating or releasing media material (i.e., words, numbers, images, or graphics) to the public. | 1,000,000 |
| **E-Crime** | |
| **Fraudulent Instruction**: This coverage protects your entity from loss resulting from the transfer, payment or delivery of money or securities as a result of fraudulent instructions provided by a third party that is intended to mislead you (e.g., social engineering techniques). | 500,000 |
| **Funds Transfer Fraud**: Coverage is provided for the loss resulting from fraudulent instructions by a third party issued to a financial institution directing such institution to transfer, pay or deliver money from your account(s). | 500,000 |
| **Telephone Fraud**: This coverage protects your organization from loss resulting from a third-party gaining access to and using your organization's telephone system in an unauthorized manner. | 500,000 |
| **Criminal Reward**: Any amount offered or paid by your organization with our prior written consent for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to your coverages. | 25,000 |
| | |
| **Aggregate Limit of Insurance** | 1,000,000 |
| **Deductible** | **See Endorsement** |