Cyber Coverage Overview

With claims examples!

As of April 2021

US & Canada Cyber Practice
## Cyber Coverage Parts

### First party coverage with claims examples

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>COVERED COSTS</th>
<th>CLAIMS EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First Party Cover</strong></td>
<td>1st Party Insurance coverage: direct loss and out of pocket expense incurred by insured</td>
<td></td>
</tr>
</tbody>
</table>
| **Business Income/ Extra Expense** | Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses. | • Loss of Income  
• Costs in excess of normal operating expenses required to restore systems  
• Forensic expenses  
• Dependent business interruption | • Malware gets into the computerized factory controllers causing the line to cease operating. IT forensics must be performed to restore system operations.  
• During routine network patching duties, an IT employee accidentally crashes the critical IT infrastructure causing operational disruption when the IT systems are inaccessible.  
• A supplier you depend for delivery of your end service to customers suffers a cyber event that prevents them from delivering critical parts/services to you. You sustain a business income loss. |
| **Data Asset Protection** | Costs to restore, recreate, or replace electronic data and other digital / intangible assets that are corrupted or destroyed. | • Restoration of corrupted data  
• Vendor costs to recreate lost data | • After a cyber event that impairs your IT (or OT) network, costs are incurred to hire an IT forensics firm to determine whether the information can be restored. The data is recreated and restored. |
| **Event Management / Breach Response** | Costs incurred responding to a network security or privacy breach. | • Forensics  
• Notification  
• Credit Monitoring  
• Call Center  
• Public Relations | • You suffer a data breach and incur costs ranging from IT forensic analysis, legal advice, costs to notify affected parties, credit monitoring for affected parties, and public relations assistance to help restore public trust in your firm. |
| **Cyber Extortion** | Costs associated with a ransomware event, regardless of whether or not a ransom demand is paid. | • Negotiation & ransom payments  
• Forensics  
• Investigation | • Your employee unwittingly clicks a link in a phishing email resulting in ransomware locking out your ability to utilize business critical technology until a ransom demand is paid (or you’re able to restore your network from back-ups). |

Note: Additional 1st party coverage like Reputational Harm, Bricking and full supply chain contingent interruption may be available.
# Cyber Coverage Parts

## Third party coverage with claims examples

<table>
<thead>
<tr>
<th>Description</th>
<th>Covered Costs</th>
<th>Claims Examples</th>
</tr>
</thead>
</table>
| **Third Party Cover**  
3rd Party insurance coverage: defense and liability costs due to alleged harm caused to others by the insured. |  
| **Privacy / Network Security Liability**  
Failure to prevent unauthorized access / disclosure of personally identifiable or confidential information; Failure of system security to prevent or mitigate a computer attack | • Liability and defense  
• Bank lawsuits  
• Consumer lawsuits | • A breach of your computer network leads to loss of sensitive customer information. Customers file suit against you for the failure to protect their private data.  
• Your network security fails to prevent a self-propagating malware from being transmitted from your network to a third party. You are suited for financial damages incurred by 3rd parties, like banks that incurred costs to re-issue bank cards to impacted individuals. |
| **Privacy Regulatory Defense Costs & PCI Fines & Penalties**  
Investigations and related fines or penalties assessed by Regulators or for violation of PCI data security standards | • Liability and defense  
• PCI / PHI / regulatory fines and penalties  
• Prep costs to testify before regulators | • A data breach leads to an investigation by a regulator such as the Office Of Civil Rights (OCR) for a breach of sensitive healthcare information leading to a HIPAA violation  
• A EU data protection authority investigates a potential GDPR violation. |
| **Media Liability**  
Including but not limited to: libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc. | • Liability and defense | • You are sued by a competitor when your CEO posts disparaging comments about the competitor on a social media site. |
| **Tech E&O**  
Acts, errors or omissions in the performance of technology services to others for a fee; or the failure of technology products to perform as intended – resulting in a financial loss. | • Liability and defense | • There is an error in the code that runs your hardware product which prevents it from operating properly. Because your customer cannot use the product, they sue you for breach of contract and other financial damages. |
Understanding scope of coverage

Insurance explained

**1st Party**
*Triggered upon discovery of an event*

Event management / breach response
Forensics, public relations, call center, notification and credit monitoring services

Business / network interruption
Extra expense and loss of business income

Cyber extortion / ransomware
Investigation, negotiation and ransom payments

Data restoration
Costs to replace, restore, recreate damaged or lost data

**3rd Party**
*Triggered by a demand/lawsuit*

Privacy Liability
Failure to prevent unauthorized access / disclosure of personally identifiable or confidential information

Network Security Liability
Failure of system security to prevent or mitigate a computer attack

Regulatory Defense and Penalties
Investigations and related fines or penalties assessed by Regulators

Technology Errors & Omissions
Allegations of negligence in provision of technology services and related products to others for a fee
Insurable Cyber Risks

- Loss or Damage to Others for Computer Security Breaches
- Legal Liability to Others for Privacy Breaches of Confidential Information
- Extra Expense to Recover/Respond to a Computer Attack
- Loss of Revenue Due to a Computer Attack
- Loss or Damage to Data/Information
- Electronic Content
- Cyber-Terrorism
- Costs to Investigate and Notify Others of a Breach
- Regulatory Actions, Fines and Scrutiny
- Cyber-Extortion
# Ransomware scenario

How an event unfolds, common missteps, and insurable costs.

## Ransomware encrypts data and network – seizing systems and disrupting / halting operations

When a company is hit by a ransomware attack, it can be a catastrophic event. The company's systems are locked, and sensitive data is encrypted. The company must decide whether to pay the ransom to decrypt the data, or to try to recover from the attack through other means.

## Company implements contingency plans and remediation steps

The company must have contingency plans in place to respond to a ransomware attack. These plans should include procedures for identifying and containing the attack, as well as plans for restoring systems and data.

## Company retains counsel and computer forensic experts

The company should retain legal counsel and computer forensic experts to help with the investigation and response to the ransomware attack. These experts can help identify the malware strain and recovery options, as well as assist with decrypting data.

## Forensic experts identify the malware strain and recovery options. Data exfiltration is confirmed. Ransom negotiation takes place simultaneously.

Computer forensic experts are crucial in identifying the malware strain and potential recovery options. Data exfiltration is confirmed, and ransom negotiation takes place simultaneously.

## To pay or not to pay? Ransom settlement is made. (The specialized experts will have a cryptocurrency wallet to make ransom payments)

The company must decide whether to pay the ransom to decrypt the data. If the ransom is paid, the specialized experts will use a cryptocurrency wallet to make the payment.

## Decryption key is obtained after ransom is paid. Computer forensic experts assist with decrypting data and recovery process

Once the ransom is paid, the decryption key is obtained and can be used to decrypt the data. Computer forensic experts can assist with the recovery process.

## Operations resume, but recovery process takes weeks – scrubbing systems, restoring network & data, forensics, etc.

After the data is decrypted, the company can begin the process of restoring systems and data. This process can take weeks, as the company must scrub systems and restore data and perform forensics.

## Common missteps

- **Event is 7pm on a Friday (unfortunately, not in client’s control!):** Incident response plans haven’t been tested against ransomware and rollout is poor. CISO can’t be reached, initial assessment can’t be performed.
- **Incident response plans haven’t been tested against ransomware and rollout is poor. CISO can’t be reached, initial assessment can’t be performed.**
- **Client does not have retainers with any incident response vendors, so in a panic, hires expensive forensic investigators from a Google search and white-shoe law firm/breach coach.**
- **Client forgets to run OFAC check on bad actor group prior to paying the demand.**
- **Client unknowingly destroyed evidence in an effort to “fix” the problem.**
- **Client’s business continuity / crisis management plans have been implemented, but didn’t consider a ransomware event.**

## Cyber insurance policy is triggered as a result of “security failure”.

- **Policy reimburses reasonable extra expenses incurred as well as business interruption loss as a result of ransomware.**
- **Policy reimburses costs for retained outside counsel and computer forensic experts. Any privacy-related costs – both first and third party – are also covered as a result of the data exfiltration.**
- **Cost of ransom is covered under the policy.**
- **Policy reimburses cost incurred for data restoration, costs to recreate and restore data.**
- **Policy may also reimburse cost for forensic accounting and preparation of proof of loss.**

## In the event there is a 3rd party liability claim, the policy reimburses defense costs and damages. Coverage can be added for bricking of hardware and reputational loss.

The policy also reimburses legal costs as a result of regulatory investigation and regulatory fines and penalties, where insurable by law, as a result of a ransomware attack.

Key exclusions that could apply in a ransomware loss could be “betterment” (systems will be brought back to where it was before the incident, but not costs to improve IT systems) and internal costs.
## Coverage Gap Analysis

### Example: business interruption and extra expense

<table>
<thead>
<tr>
<th>Cyber Peril</th>
<th>Property</th>
<th>Special Crime</th>
<th>Commercial Crime</th>
<th>General Liability</th>
<th>Traditional Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Party – Direct costs and out of pocket expenses incurred by the insured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business interruption - security failure</td>
<td>Small sublimit, if included</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business interruption - system failure / administrative error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dependent business interruption (supplier/IT outsourcer) – security failure</td>
<td>Small sublimit, if included</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dependent business interruption (supplier/IT outsourcer) – system failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voluntary shutdown</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data asset restoration</td>
<td>Small sublimit, if included</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extra expense</td>
<td>Small sublimit, if included</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies.
Defining Cyber Risk

“The possibility of loss or injury of, relating to, or involving data or technology”

What is Data?

- Factual information (such as measurements or statistics) used as basis for reasoning, discussion, or calculation
- Information in digital form that can be transmitted or processed
- Information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful

What is Technology?

- Computer Systems and networks, including cloud and data storage
- Electronic devices, such as sensors, that are embedded in everyday objects or machinery and enable them to send and receive data, and/or to connect to internet (aka Internet of Things or IoT devices)
- Automated machinery and equipment that can be controlled or programmed by computers
- Computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation (aka Artificial Intelligence or AI)
Impacts & consequences of cyber events
And silent cyber implications

Cyber Event
Malicious attacks or accidental events to your digital system (incl. IT & OT), data (in house or outsourced), or technology

Impact
Non-physical
Confidentiality issues
Integrity issues
Availability issues

Physical
Property Damage
Bodily Injury

Consequence
Leading to losses/claims:
Loss of Income
1st Party Costs
3rd Party Liability
Fines & Penalties
Extortion Demands
Negligence in Services
Shareholder Litigation

Marsh
Mind the Gap

The intersection between cyber risk and physical risk is “physical cyber risk”. Broad “silent cyber” exclusions create a gap in cover for physical cyber risk.
Appendix
Coverage Descriptions without claims examples
Why buy cyber?
# Cyber Coverage Parts

## First Party Coverages

<table>
<thead>
<tr>
<th>First Party Cover</th>
<th>DESCRIPTION</th>
<th>COVERED COSTS</th>
</tr>
</thead>
</table>
| **Business Income/ Extra Expense** | Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses. | • Loss of Income  
• Costs in excess of normal operating expenses required to restore systems  
• Dependent business interruption  
• Forensic expenses |
| **Data Asset Protection** | Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed. | • Restoration of corrupted data  
• Vendor costs to recreate lost data |
| **Event Management / Breach Response** | Costs resulting from a network security or privacy breach. | • Forensics  
• Notification  
• Credit Monitoring  
• Call Center  
• Public Relations |
| **Cyber Extortion** | Costs associated with a ransomware event, regardless of whether or not a ransom demand is paid. | • Forensics  
• Investigation  
• Negotiations and payments of ransoms demanded |
## Cyber Coverage Parts
### Third Party Coverages

<table>
<thead>
<tr>
<th>Third Party Cover</th>
<th>DESCRIPTION</th>
<th>COVERED COSTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third Party Cover</strong></td>
<td>3rd Party insurance coverage: defense and liability incurred due to alleged harm caused to others by the insured.</td>
<td></td>
</tr>
</tbody>
</table>
| **Privacy Liability** | Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach. | • Liability and defense  
  • Bank lawsuits  
  • Consumer lawsuits |
| **Network Security Liability** | Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use. | • Liability and defense |
| **Privacy Regulatory Defense Costs & PCI Fines & Penalties** | Privacy breach and related fines or penalties assessed by Regulators. | • Liability and defense  
  • Investigation by a regulator  
  • Prep costs to testify before regulators  
  • PCI / PHI fines and penalties |
| **Media Liability** | Defense and liability for, including but not limited to, libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc. | • Liability and defense |
Why are organizations buying cyber insurance?

- Escalation of cyber attacks impacting operations, including supply chain risk. Shift of corporate balance sheets away from ‘hard assets’ to digital assets. Significant increase in ransomware.
- Cyber risk now a top priority on the Executive Branch risk agenda
- State, Federal and Global Regulatory Requirements
- Litigation and Contractual obligations
- Growing recognition that the consequences of a cyber incident necessitate cyber risk transfer and operational resilience planning
- Broad coverage and service offerings; coupled with coverage restrictions in the traditional P&C markets (i.e. silent cyber)
We are leaders in risk, strategy and people. One company, with four global businesses, united by a shared purpose to make a difference in the moments that matter.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are intended solely for the entity identified as the recipient herein ("you"). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. All decisions regarding the amount, type or terms of coverage shall be your ultimate responsibility. While Marsh may provide advice and recommendations, you must decide on the specific coverage that is appropriate for your particular circumstances and financial position. By accepting this report, you acknowledge and agree to the terms, conditions, and disclaimers set forth above.

Copyright © 2021 Marsh LLC. All rights reserved.