Coalition®

BROUGHT TO YOU IN PARTNERSHIP WITH RPS RISK PLACEMENT SERVICES

CYBER INSURANCE REIMAGINED

Introducing the most innovative and comprehensive coverage available.

We found existing cyber insurance policies lacking, so we created our own. Full limits, enhanced business interruption cover, protection from physical cyber attacks, computer replacement coverage (an industry first—only available through Coalition), and more.

3rd Party Liability Coverages

Network & Information Security Liability **Regulatory Defense & Penalties** **Multimedia Content Liability** **PCI Fines & Assessments**	We cover the expenses to defend you and any damages resulting from your liability to a 3rd party, or for regulatory fines & penalties, multimedia wrongful acts (such as infringement, defamation, piracy, etc.), and PCI fines & assessments resulting from a failure in your security, data breach, or privacy violation.
Bodily Injury & Property Damage **Technology Errors & Omissions**	We pay for the costs of defense and damages from your liability to a 3rd party when a failure in your security results in physical damage or injury.

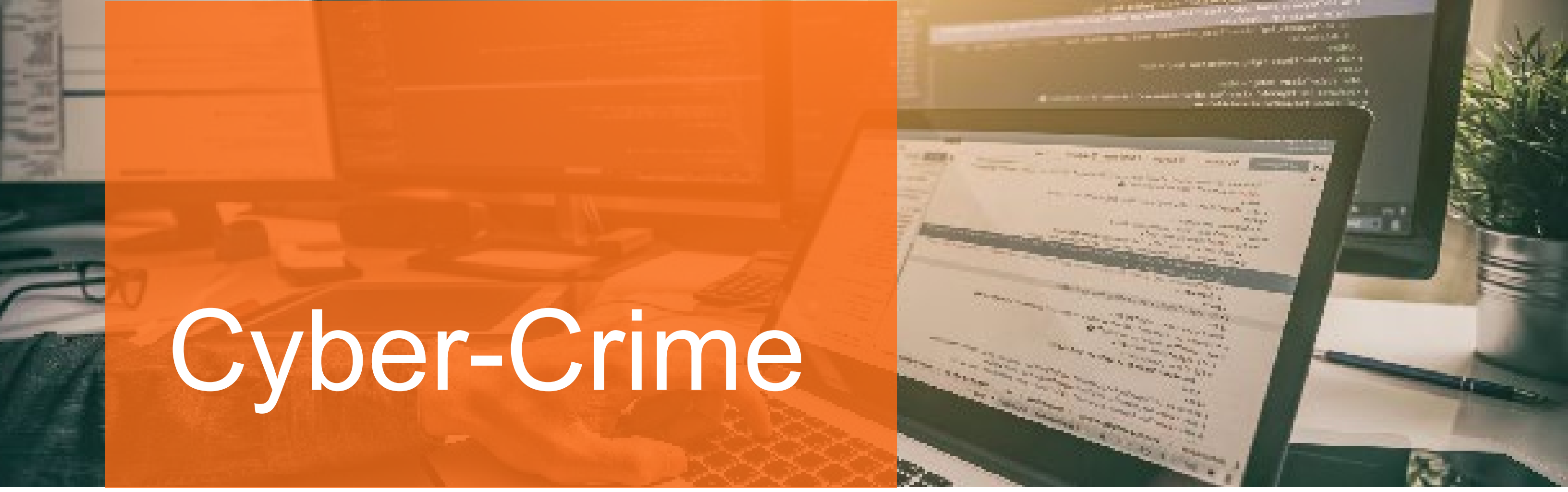
1st Party Loss Coverages

Bodily Injury & Property Damage **Pollution**	In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution.
Computer Replacement	We cover the costs to replace your computer systems that are permanently impacted by malware.
Fund Transfer Fraud	We pay for funds transfer losses you incur from a failure in your security or social engineering.
Service Fraud	We pay for the additional amounts you're billed by a cloud or telephone provider when you incur fraudulent charges.
Digital Asset Restoration	We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a failure of your security.
Business Interruption & Extra Expenses	We cover financial losses resulting from a failure in your security, data breach, and even systems failure (including contingent/dependent BI), as well as the extra expenses you incur to bring your company back online.
Cyber Extortion	We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.
Breach Response **Crisis Management & Public Relations**	We pay for the costs to respond to a breach including 3rd party incident response and public relations experts, customer notification costs and credit monitoring, media purchases, and legal fees; and advise in connection with the incident, among others.

Not all insurance policies are equal

Coverage	Coalition	Others
Business Interruption & Extra Expenses	✔ See enhancements below[1]	✘ Sometimes
Contingent Business Interruption	✔	✘
Funds Transfer Fraud	✔	✘ Sometimes (sublimited)
Cyber Extortion	✔	✘ Sometimes
Computer Replacement	✔	✘
Bodily Injury & Property Damage	✔	✘
Pollution	✔	✘
Service Fraud	✔ See enhancements below[2]	✘
Network & Information Security Liability	✔	✔
Regulatory Defense & Penalties	✔	✔
Multimedia Content Liability	✔ See enhancements below[3]	✔
PCI Fines & Assessments	✔ No sublimit	✔ Sublimited
Digital Asset Restoration	✔ See enhancements below[4]	✔
Breach Response	✔	✔
Crisis Management & Public Relations	✔ See enhancements below[1]	✔

Enhancements	Coalition	Others
Pre-claims assistance	✔	✘
Covers all prior acts	✔	✘ Sometimes
Systems failure[1]	✔	✘
Waiting period[1]	✔ As low as 1 hour	✘ 8+ Hours
Business services costs[2]	✔	✘
Cost of system upgrades[4]	✔	✘
Reputation Repair[5]	✔	✘
BYOD coverage	✔	✘
Social media / IoT coverage[3]	✔	✘ Sometimes
Cybersecurity apps	✔	✘



Cyber-Crime

At RPS, we have observed that cyber-crime loss remains one of the most common claims. Unfortunately, many crime policies lack coverage for cyber-crime or have limitations that leave clients vulnerable. Additionally, the language used in each carrier's form can create gaps in coverage. Our team is dedicated to finding the best coverage form for your client's specific needs.

Our Cyber-Crime coverages include:

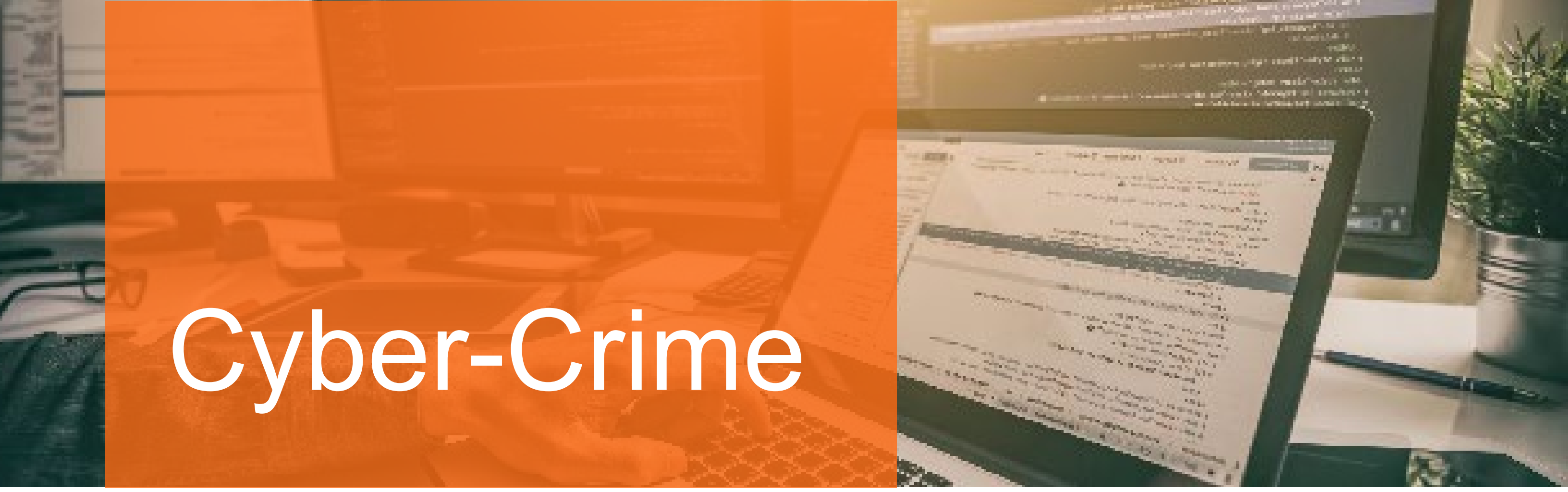
- **Social Engineering/Fraudulent Instruction/Cyber Deception:** This coverage protects against the loss of money or tangible property resulting from fraudulent requests, including theft of funds held in escrow.
- **Invoice Manipulation:** This coverage indemnifies the insured for direct net loss caused by the inability to collect payment via invoice.
- **Funds Transfer Fraud:** This coverage protects against the loss of money or securities resulting from fraudulent instructions to a financial institution.
- **Theft of Funds in Escrow:** This coverage safeguards against the electronic theft of client funds held by the insured.
- **Push Payment Fraud/Phishing Fraud:** This coverage addresses the inability to collect payment or outstanding account receivables due to a cyber-incident.

When considering cyber-crime coverage, it is important to assess the following:

- Does the insured have exposure to sending "property"? Some social engineering coverage only covers "money," but certain forms extend coverage to include "property" and "goods."
- Does the insured have exposure to holding client funds? Most forms do not cover the insured for holding client funds.
- Does the insured have both a crime and cyber policy with similar cyber-crime coverages? It is crucial to ensure that both policies have the appropriate policy wording to respond as primary and/or excess to each other.

To illustrate the importance of cyber-crime coverage, consider the following scenarios:

- **Social Engineering Scenario:** A vendor's email account is breached, and the insured is persuaded to change banking and account information. As a result, the insured pays $50,000 to the new banking information, which turns out to be an offshore account for the perpetrator.
- **Invoice Manipulation Scenario:** Hackers gain access to the insured's system and send fraudulent invoices to customers, redirecting funds to their own account. Although customers pay the invoices, the insured is unable to collect.
- **Funds Transfer Fraud Scenario:** An unauthorized third party impersonates the insured and instructs the insured's bank to transfer funds to an offshore account.



Cyber-Crime

To prevent cyber-crime, we recommend the following best practices:

1. Educate employees on how to recognize and handle phishing emails through security awareness training programs.
2. Implement a Secure Email Gateway (SEG) to prevent spam, phishing, and malicious emails from reaching employees' inboxes.
3. Enforce Multi-Factor Authentication (MFA) on email accounts to prevent unauthorized access and fraudulent funds transfer requests.
4. Train employees to validate and verify payment requests directly with the vendor or requestor using a trusted phone number, rather than relying on information provided in emails.
5. Include response steps in your Incident Response Plan to effectively address funds transfer fraud, including reporting to company management, the bank, law enforcement, and your insurance carrier.

Contact us for a quote today.

Insurance Masters, Inc.
Michael M. Berman
5388 Dunteachin Drive
Ellicott City, MD 21043-8204

410.971.5869 Phone/Text
MTBERMAN@MSN.com
New Website: InsuranceMastersInc.com

RISK PLACEMENT SERVICES