

RPSCyber FAQs



Risk Placement Services, Inc.

Knowledge. Relationships.
Trust and Confidence.

WHAT IS CYBER LIABILITY INSURANCE?

“Cyber” Liability is insurance coverage specifically designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private
- Liability claims alleging personal injury and/or intellectual property violations in a digital, online or social media environment
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.
- Defense costs in State or Federal regulatory proceedings that involve violations of privacy law; and
- The provision of expert resources and monetary reimbursement to the Insured for the out-of-pocket (First-Party) expenses associated with the appropriate handling of the types of incidents listed above

The term “Cyber” implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats—paper, digital or otherwise.

WHAT DOES PRIVACY LIABILITY COVER?

The Privacy Liability insuring agreement in our policy goes beyond providing liability protection for the Insured against the unauthorized release of Personally Identifiable Information (PII), Protected Health Information (PHI), and corporate confidential information like most popular “Data Breach” policies. Rather, our policy provides true “Privacy” protection in that the definition of Privacy Breach includes violations of a person’s right to privacy, publicity, etc. Because information lost in every data breach may not fit State or Federal-specific definitions of PII or PHI, our policy broadens coverage to help fill these potentially costly gaps. This is a key provision that truly sets the RPS policy apart from others.

*Knowledge,
Relationships,
Trust and
Confidence.*

WHAT DOES PRIVACY REGULATORY CLAIMS COVERAGE COVER?

The Privacy Regulatory Claims Coverage insuring agreement provides coverage for both legal defense and the resulting fines/penalties emanating from a regulatory claim made against the Insured, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation with respect to privacy regulations.

WHAT DOES SECURITY BREACH RESPONSE COVERAGE COVER?

This First-Party coverage reimburses an Insured for costs incurred in the event of a security breach of personal, nonpublic information of their customers or employees. Examples include:

- The hiring of a public relations consultant to help avert or mitigate damage to the Insured’s brand
- IT forensics, customer notification and First-Party legal expenses to determine the Insured’s obligations under applicable Privacy Regulations
- Credit monitoring expenses for affected customers

Our policy can extend coverage even in instances where there is no legal duty to notify if the Insured feels that doing so will mitigate potential brand damage (such voluntary notification requires prior written consent).

WHAT DOES SECURITY LIABILITY COVER?

The Security Liability insuring agreement provides coverage for the Insured for allegations of a “Security Wrongful Act,” including:

- The inability of a third party, who is authorized to do so, to gain access to the Insured’s computer systems
- The failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as “phishing” that results in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party
- Protects against liability associated with the Insured’s failure to prevent transmission of malicious code from their computer system to a third party’s computer system



Orange Insurance & Bonding

• SMALL BUSINESS SPECIALISTS •

☎ 877.288.6103 ✉ info@orangeinsurance.com 🌐 www.orangeinsurance.com

WHAT DOES MULTIMEDIA LIABILITY COVER?

The Multimedia Liability insuring agreement provides broad coverage against allegations that include:

- Defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the Insured's communication of media content in electronic (website, social media, etc.) or nonelectronic forms

Other "Cyber" insurance policies often limit this coverage to content posted to the Insured's website. Our policy extends what types of media are covered as well as the locations where this information resides.

WHAT DOES CYBER EXTORTION COVER?

The Cyber Extortion insuring agreement provides:

- Expense and payments to a harmful third party to avert potential damage threatened against the Insured such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information.

WHAT DOES BUSINESS INCOME AND DIGITAL ASSET RESTORATION COVER?

The Business Income and Digital Asset Restoration insuring agreement provides for lost earnings and expenses incurred because of a security compromise that leads to the failure or disruption of a computer system, or, an authorized third-party's inability to access a computer system. Restoration costs to restore or recreate digital (not hardware) assets to their preloss state are provided for as well. What's more, the definition of Computer System is broadened to include not only systems under the Insured's direct control, but also systems under the control of a Service Provider with whom the Insured contracts to hold or process their digital assets.

WHAT IS "PCI-DSS ASSESSMENT" COVERAGE?

The Payment Card Industry Data Security Standard (PCI-DSS) was established in 2006 through a collaboration of the major credit card brands as a means of bringing standardized security best practices for the secure processing of credit card transactions. There are six stated goals and 12 requirements that merchants and service providers must adhere to in order to be "PCI Compliant." The RPS Cyber Policy can help offset the cost of damages and claim expenses that the Insured becomes legally obligated to pay for when there are violations of this agreement in the wake of a breach involving cardholder data.

HOW IS THIS POLICY BETTER THAN OTHER OPTIONS IN THE MARKETPLACE?

As with any insurance policy, what sets our coverage apart lies in the definitions and exclusions in the policy. The RPS Cyber Policy offers broader definitions of critical terms such as Privacy Breach, Computer System, and Media Content. These definitions, along with the absence of some industry-standard exclusions and a drastically streamlined application process, make this policy

more comprehensive and easier to access than the typical cyber policy available from traditional sources. A high-level cyber policy comparison can be found here that comparatively demonstrates the advantages of our form over other cyber policies.

ISN'T THIS ALREADY COVERED UNDER MOST BUSINESS INSURANCE PLANS?

The short answer is "No." While liability coverage for data breach and privacy claims has been found in limited instances through General Liability, Commercial Crime and some D&O policies, these forms were not intended to respond to the modern threats posed in today's 24/7 information environment. Where coverage has been afforded in the past, carriers (and the ISO) are taking great measures to include exclusionary language in form updates that make clear their intentions of not covering these threats. Additionally, even if coverage can be found in rare instances through other policies, they lack the expert resources and critical First-Party coverages that help mitigate the financial, operational and reputational damages a data breach can inflict on an organization.

HOW DO I EDUCATE MY CLIENTS ABOUT THEIR NEED FOR THIS COVERAGE?

RPS has developed several tools to help your clients understand their need for this critical coverage. We periodically conduct client-focused webinars where agents can invite their clients and one-page sell sheets can be downloaded here to include with your proposals. If you have a larger opportunity and need a Cyber Liability professional to talk to your client or prospect via phone or online meeting, just call your preferred RPS Cyber professional.

ARE BUSINESSES REQUIRED TO CARRY THIS COVERAGE?

While there is presently no law that requires a business or organization to carry Cyber Liability, there is a national trend in business contracts for proof of this coverage. In addition, the SEC is encouraging disclosure of this coverage as a way of demonstrating sound information security risk management. Laws such as HIPAA-HITECH and Gramm-Leach-Bliley and state-specific data breach laws are continually driving demand as requirements for notification in the wake of a data breach become more expensive.

DO SMALL BUSINESSES NEED THIS COVERAGE?

The Symantec 2014 Internet Security Threat Report reports that small businesses accounted for 30% of targeted spear-phishing attacks in 2013. In 2012, Verizon reported that approximately 40% of all data breaches that year occurred among companies with fewer than 100 employees. Even more alarming is the fact that 60% of companies that have been a victim of cyber-attacks are out of business within six months. While breaches involving public corporations and government entities garner the vast majority of headlines, it is the small business that can be most at risk. With lower information security budgets, limited personnel and greater system vulnerabilities, small businesses are increasingly at risk for a data breach.

RPSCyber FAQs

IF E-COMMERCE FUNCTIONS SUCH AS PAYMENT PROCESSING OR DATA STORAGE ARE OUTSOURCED, IS THIS COVERAGE STILL NEEDED?

The responsibility to notify customers of a data breach or legal liabilities associated with protecting customer data, remain the responsibility of the Insured. Generally speaking, business relationships exist between Insureds and their customers, not their customers and the back-office vendors the Insured uses to assist them in their operations. Outsourcing business critical functions, such as payment processing, data storage, website hosting, etc., can help insulate Insureds from risk; however, the contractual agreement wording between Insureds, their customers and the vendors with whom they do business will govern the extent to which liability is assigned in specific incidents.

WHAT IS THE COST OF NOT BUYING THE COVERAGE AND SELF-INSURING A DATA BREACH?

The Ponemon Institute, a well-known research firm, publishes an annual “Cost of a Data Breach” report. In partnership with IBM, the 2014 report indicated that the average cost paid for each lost or stolen record is \$201. These numbers are reflective of both the indirect expenses associated with a breach (time, effort and other organizational resources spent during the data breach resolution, customer churn, etc.), as well as direct expenses (customer notification, credit monitoring, forensics, hiring a law firm, etc.).

Because every breach is different, and the per-capita cost of a breach depends largely on the number of records compromised, it is helpful for small to mid-sized organizations to start with a lower number of \$65/record, (the average direct costs associated with a breach in the Ponemon study)—multiply this number by the estimated number of records containing PII, PHI or financial account information in the Insured’s control. By engaging in this simple exercise, businesses quickly understand the financial value of implementing cyber insurance as a risk transfer vehicle. More information can be found at www.ponemon.org.

WHO IS THE INSURANCE CARRIER?

For non-admitted states, the RPS Cyber Policy is written on an excess and surplus lines (non-admitted) basis on Lloyd’s of London paper. The policy is secured equally through Barbican Consortium 9354, Brit Syndicate 2987 and Aegis Consortium 9937. Lloyd’s of London has received an A.M. Best’s A (Excellent) XV rating and has the claims-paying stability of Lloyd’s. The following states are currently non-admitted: VT, CT, NY, NJ, NC, SC, FL, IN, and MN.

For admitted states (all states other than those listed above), the BCS Cyber and Privacy Liability Policy is underwritten by BCS Insurance Company and powered by and with the backing of certain syndicates at Lloyd’s of London. BCS Insurance Company is a licensed insurance company in all states, Puerto Rico and the District of Columbia. BCS Insurance Company provides value through a solid foundation of strong governance, national and international capabilities and product and industry expertise, and

is rated A- (Excellent) IX by A.M. Best. BCS Insurance has been in business for over 60 years. It is a wholly owned subsidiary of BCS Financial Corporation which, in turn, is owned by all Blue Cross Blue Shield primary licensees. BCS Insurance Company’s relationship with certain syndicates at Lloyd’s of London brings additional strength, stability and industry leading expertise to the cyber insurance program.

ARE TAXES AND FEES IN ADDITION TO THE STATED PREMIUM SHOWN IN THE QUOTE?

Yes. For policies issued in non-admitted states, the Insured will be responsible for paying state-specific surplus lines taxes and fees and a nominal RPS fee. These fees will be detailed specifically in the bill you receive from RPS. Please be sure to let your client know that the premium indicated in the quotation is not inclusive of these taxes and fees, and the precise premium (inclusive of all taxes and fees) will be sent to them via invoice by you.

HOW IS PAYMENT PROCESSED IF BOUND THROUGH THIS ONLINE SYSTEM?

The process is quite simple. When you enter a new quote into the system, a premium will be generated with the quotation (exclusive of surplus lines taxes and fees). Once you bind coverage, you will receive an invoice from RPS that reflects the premium, plus surplus lines taxes and fees, and any applicable RPS fees. From there, you will bill your client, collect payment, and pay RPS the full amount, less the applicable agency commission, within 30 days of binding.

WHAT IS THE CLAIMS-HANDLING PROCESS?

Insureds have available a 24-hour data breach hotline to report incidents or even suspected incidents. Clyde & Co. is the designated legal firm in the U.S. that has been contracted to triage initial notices in this regard. Your RPS broker will receive notification of the incident as well. It is critical to advise your clients to immediately report any and all incidents that they believe could give rise to a claim of any kind under this policy.

HOW DO I CHANGE INFORMATION ABOUT THE INSURED?

Simply locate the relevant policy by typing the policy number into the quick search box on the right side of the menu bar. When you see the policy screen, click the “Mid Term Policy Adjustment” button and select “Client Data Change.” Insert the updated data in the fields provided.

IS IT POSSIBLE TO RENEW THIS POLICY ONLINE?

Yes. Simply locate the relevant policy by typing the policy number into the quick search box on the right side of the menu bar. Once on the policy screen you will see one of two alternative buttons—“Renew” or “Back to Quote Stage.” Click the “Renew” button for policies within 30 days of the renewal date. The “Back to Quote Stage” button will be available for policies that are not within 30 days of the renewal date. By selecting “Back to Quote Stage,” a new quote will be provided and will be valid for up to 60 days. Click on the appropriate button and follow the instructions.