Frequently Asked Questions

Do you have any questions about your insurance? The frequently asked questions below are here to help you make an informed decision.

What is Cyber Liability Insurance?

"Cyber" Liability is insurance coverage specifically designed to protect a business or organization from a range of threats and incidents relating to a breach event including:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private
- Liability claims alleging invasion of privacy and/or copyright/trademark 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 (1st 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 (including Employee Privacy) and Security Liability cover?

The Privacy Liability aspect of the 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.

The Security Liability part of the 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

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.

Does this policy cover regulatory investigations and/or fines related to GDPR privacy violations?

The BCS cyber policy has always provided broad Regulatory Claim coverage that would contemplate defense and penalties associated with unintentional violations of domestic and foreign privacy statutes. In accordance with the implementation of the EU's General Data Protection Regulation, BCS added clarifying language to the policy form under the definitions of Privacy Regulations and Private Information to specifically reference coverage for GDPR by name (subject to policy terms and conditions). It is important to note that fines and penalties may not be insurable by law in certain U.S. States and in certain foreign countries, including some member countries of the European Union.

What does Security Breach Response Coverage cover?

This 1st Party coverage reimburses an Insured for costs incurred in the event of a security breach of personal, non-public 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 1st Party legal expenses to determine the Insured's obligations under applicable Privacy Regulations
- Credit monitoring expenses for affected customers for up to 12 months, and longer if circumstances require.

Our policy can also 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 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 non-electronic 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. The policy will also cover for lost business as a result of a loss of reputation caused by any failure or disruption to computer systems. Restoration costs to restore or recreate digital (not hardware) assets to their pre-loss 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. Merchants and service providers must adhere to certain goals and requirements in order to be "PCI Compliant," and certain specific agreements, may subject an Insured to an "assessment" for breach of such agreements. The RPS Cyber Policy responds to PCI assessments as well as claims expenses in the wake of a breach involving cardholder information.

What is Cyber Deception coverage?

The Cyber Deception extension is purchased for an additional premium if the applicant is eligible. The extension provides coverage for the intentional misleading of the Applicant by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the Applicant believing it to be genuine. This is commonly known as "spear-phishing" or "social engineering".

What is Telephone Hacking coverage?

Telephone Hacking coverage is included in the **Electronic Fraud** sub-section of the Gallagher policy. It provides a sub-limit of coverage for the intentional, unauthorized and fraudulent use of your **Telecommunications Services** (ie: telephone, fax, broadband or other data transmission services that you purchase from third parties) that results in unauthorized calls or unauthorized use of your bandwidth.

What is Funds Transfer Fraud coverage?

Funds Transfer Fraud coverage is available in the **Electronic Fraud** sub-section of the Gallagher policy for insureds who are NOT classified as Financial Institutions (Financial Institutions includes Community, State or Credit Unions, as well as National financial institutions, banks, etc.) For those organizations who are not in the financial institution classification, the coverage provides coverage for unauthorized electronic funds transfer, theft of your money or other financial assets from your bank by electronic means, theft of your money or other financial assets from your corporate credit cards by electronic means, or any fraudulent manipulation of electronic documentation while stored on your **Computer System.** This should not be confused with **Cyber Deception** coverage which requires a willful release of funds (not theft) based on a fraudulent instruction the insured believes to be true.

Who is RPS?

With more than 1,000 employees in more than 30 U.S. States, Risk Placement Services empowers insurance agents and brokers like yours with product and industry expertise, and access to exclusive Property & Casualty insurance coverage for their clients throughout the country. RPS is the exclusive Managing General Agent for the specialized Cyber insurance quotation your agent has provided herein. RPS is consistently recognized by Business Insurance magazine as the nation's largest Managing General Agency. Your agent's decision to partner with RPS speaks of their desire to provide your organization with the best insurance solutions available in the marketplace today.

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.

Further strengthening our offering is that claims under Insuring Clause A - Privacy Liability (including Employee Privacy) and Security Liability; and Insuring Clause B – Privacy Regulatory Claims Coverage are both subject to an each and every claim limit, and are not restricted by the policy aggregate, even if you experience multiple cyber incidents during the same policy period.

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 1st Party coverages that help mitigate the financial, operational and reputational damages a data breach can inflict on an organization.

Are businesses required to carry this coverage?

While there is presently no law that requires a business or organization to carry Cyber Liability Insurance, 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, GDPR, 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?

A recent Ponemon Institute report uncovered that 50% of small and medium sized US businesses had suffered a data breach, with 55% suffering a cyber-attack, with the most prevalent attack being non-sophisticated phishing attempts. The US National Cyber Security Alliance has advised that 60% of small companies are out of business within 6 months after being hacked. 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.

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 <u>not</u> 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 2017 report indicated that the average cost paid for each lost or stolen record is $141. 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.).

While there has been a decrease in the average cost paid for each lost or stolen record since 2016, (down from $158), the average size of a breach has increased to 1.8 times the size of breaches last year. So, despite decreasing average costs per record, more records are being lost which means an increasing cost to businesses. More information can be found at www.ponemon.org.

In addition, the cost of breaches has evolved from just the cost of notification to now include ransom demands, business income loss, theft, and associated liability costs. These additional factors have also contributed to driving up the potential financial impact of a breach incident.

Who is the insurance carrier?

The RPS Cyber Policy is written on an excess and surplus lines (non-admitted) basis on Lloyd's of London paper. The coverage has received AM Best's "A" (Excellent) rating and has the claims-paying stability of Lloyd's.

Are taxes and fees in addition to the stated premium shown in the quote?

Yes. 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. 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 you from your agent.

What is the claims-handling process?

A 24-hour data breach hotline is available to report incidents or even suspected incidents. As soon as you suspect a data breach incident or receive notice of a claim, you should call the hotline listed in your policy. This hotline is manned by Baker Hostetler, a world-wide leading privacy law firm with experience in handling thousands of data breach events. After this initial call, Baker Hostetler will then provide on your behalf the required notice to Atheria Law PC, the designated legal firm that has been contracted to triage initial notices on behalf of the insurer. Your RPS broker will receive notification of the incident (or any third-party claim) as well. It is critical that you immediately report any and all incidents that you believe could give rise to a claim of any kind under this policy. You can expect Baker Hostetler to manage all breach response related activities associated with data/privacy incidents. It is also likely that interaction with representatives from Atheria Law will occur throughout the claims process for matters concerning coverage applicability, retentions, reimbursements and payment to vendors.

What if there are questions that are not answered here?

Please contact your preferred Cyber Professional who will assist you with any questions you may have.