



Risk Placement Services, Inc.

Knowledge. Relationships.
Trust and Confidence.

Cyber Liability Insurance for Sports Organizations





The biggest threat to your organization or club isn't a loss of funds. It's a loss of data.

From online sign-ups and payment systems to social media tools for parent and team information - with advanced technology, the results are instantaneous. But, in this new digital world, while the user experience is enhanced, the risks become more significant.

As a sports program administrator, it is critical to ask yourself this question: "What would be the worst case scenario for our sports organization if the private information of our membership found its way into the wrong hands?"

Specialized insurance coverage from RPS Bollinger, a national leader in Cyber and Privacy Liability, is now available and can help protect sports teams and organizations in the following areas:

- Privacy Liability
- Privacy Notification Expense
- Regulatory Liability
- Media Content Liability
- Network Security Liability
- Crisis Management
- Credit Monitoring Expense
- E-Extortion Threat

What can go wrong?

Hacking: The Boca Ski Club in Palm Beach, CA was the victim of an attack when hackers accessed the club's membership roster and posted personal information, including names, dates of birth, addresses and email addresses, online.

[Privacyrights.org](https://www.privacyrights.org)

Intentional Data Leak: Youth League registration forms for the PAL Youth Football league of Milpitas, CA were stolen from the back seat of a coach's car. The forms included children's names, addresses, birth certificates and health insurance information.

Mercury News, San Jose, CA

Phishing Attack: The financial officer of the Oakwood Athletic Club in San Ramon, CA was the victim of a phishing attack when a hacker, purporting to be a board member, requested and received the W-2 and payroll information of the employees of the organization.

Databreach Report - CA Attorney General

Unintentional Data Leak: The prestigious Princeton Tower Club of Princeton, NJ, mistakenly attached and emailed to the membership, the names and social security numbers of their entire organization. Over 200 members of the club were notified of the breach.

[EducationNewYork.com](https://www.educationnewyork.com)

Get a Quote Today

Real life data breaches such as these are excluded from traditional insurance policies. Call or email to find out how you can partner with RPS Bollinger to protect your organization from a privacy or network security breach.

Abigail Panciello, CISR

Abigail_Panciello@RPSins.com

973.921.8080

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) 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 of third parties and employees, 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 this cyber policy apart from others.

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 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 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



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. This 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".

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. This 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.

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 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?

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 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 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 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.



How can I tell which states are on an admitted form vs a non-admitted form?

Most States are on the admitted paper and written through BCS Insurance Company. For those remaining states where the admitted filings are still in process, the forms will be written through Lloyd's of London. Currently, all states are written on admitted paper except: VT. To obtain a quote for these states, please contact your retail agent for assistance.

Who is the insurance carrier?

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) 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 this cyber insurance program.

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. Immediately after calling the hotline, you are required to send notice to Clyde & Co., the designated legal firm that has been contracted to triage initial notices in this regard. This can be done by sending an email with a brief description of the incident, including your contact information, to the claims-reporting email address listed in your policy. Your 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.

What if there are questions that are not answered here?

Please contact us at 973.921.8080 or email us Abigail_Panciello@RPSins.com and a Cyber Professional will assist you with any questions you may have.





*Knowledge.
Relationships.
Trust and Confidence.*

RPS BOLLINGER

PO Box 1322 Morristown, NJ 07960
Ph. 800.446.5311 • Fax 973.921.8474
RPSBollinger.com