Cyber Market Comparison

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Policy form version: Each policy version and year has specific terms and conditions that apply. It is important to understand which policy you will be purchasing.	94.200 (2019)	Cyber Wording Edition: January 17, 2020	AXIS Pro® Privasure™ PVSR-101 (08-16)	Hiscox CYBERCLEAR Cyber Coverage Part CYBCL-CYB P0001A CW (10/19)	Cyber, Private Enterprise CFC-CY-0037 (11/19)
Admitted policy: Admitted insurance carriers comply with each state's regulations and must file their rates with the state. Nonadmitted carriers are not licensed with the state but are allowed to transact business in the state. They do not have to file their rates and have more flexibility in the type of insurance/insureds they protect. Insureds purchasing nonadmitted insurance are also subject to the state's surplus lines taxes and fees.	✓ California-based insureds to be written on Lloyd's surplus lines paper (effective May, 2022 for renewing and new policies).	Nonadmitted Surplus lines taxes and fees apply. 60-day notice of nonrenewal is not required. 30% minimum earned premium applies.	✓	✓	✓
Full prior acts: A retroactive date eliminates coverage for wrongful acts or security events (i.e., an unknown hack or an unknown breach of a security system) that took place prior to the date specified on the policy. Full prior acts eliminate this concern.	✓	✓	✓	✓	✓
Single retention applies for each event regardless of the number of coverages: Even if a retention is shown for each insuring agreement, only one retention (the largest) will apply in case multiple insuring agreements are triggered in a cyber event.	✓	✓	✓	✓	✓
Zero dollar retention for breach/incident response counsel (BRC): If the insured elects to use the carrier's BRC for help in a covered event, no retention will apply. If no additional costs are incurred, the BRC's cost will be paid by the carrier without any out-of-pocket costs to the insured.	✓	✓			✓

RPS™ RISK PLACEMENT SERVICES

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Are sublimits applicable to cyber extortion/ ransomware coverage? If yes, is the sublimit applicable to certain industries only, or, is it applied if certain information security measures aren't taken? Also, is it applicable only to cyber extortion/ransomware, or to the entire policy (all insuring agreements)?		✓ Tied to industry (applicable to education and government industry classes only). $50,000 sublimit applies to any claims, events or losses arising from a cyber extortion threat via the cyber extortion threat sublimit endorsement. The sublimit is not merely applicable to the cyber extortion insuring agreement, it applies to the entire policy.		✓ Tied to controls. Insureds who indicate that they cannot recover all of their business-critical data and systems within 10 days will receive the ransomware event sublimit endorsement. This endorsement applies an aggregate limit of $25,000 on the entire policy, applicable to all loss arising from a ransomware event.	
Media liability coverage includes paper and electronic content: Coverage for libel, slander, plagiarism, privacy or misappropriation of ideas, infringement of copyright, domain name, trade dress, title, or slogan in the course of publishing, displaying, releasing, transmitting, or disclosing any content.	✓	✓	Website media only.	Website and social media only. This represents a narrowing of coverage via the Digital Media Liability coverage part (automatically included).	✓
Cyber deception (social engineering) coverage available: Provides coverage in the event the insured transfers the insured's funds or the insured's property to a third party that is being impersonated by another (i.e., a hacker) in an attempt to defraud the insured. Note: Certain industry classes may be ineligible for social engineering/cyber deception.	✓ $100,000 or $250,000 limits offered as options for purchase. Eligibility for coverage requires that the insured have a callback verification process when making changes to or setting up new payment instructions to a third party.	✓ $100,000 or $250,000 limits offered as options for purchase. Eligibility for coverage requires that the insured have a callback verification process when making changes to or setting up new payment instructions to a third party.	✓ Automatically included $100,000 sublimit. Does not cover property. Requires that the insured attempt to validate the request prior to sending funds.	✓ $100,000 sublimit offered as option for purchase as part of Cyber Crime coverage. Does not cover property.	✓ Automatically include $100,000 authorized push payment fraud for eligible classes of business (as part of Cyber Crime section—shared $100,000 limit). $250,000 limit option is available. Requires the insured has a funds transfer policy in place for Cyber Crime insuring clause to apply (requirement of employee training on the funds transfer policy, and the requirement to verify the validity of the request via contact information and a method that is different from the method the communication is received by).
Cyber deception (social engineering): Covers the loss of the insured's funds, as well as funds they hold on behalf of others.	✓	✓			✓

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Telecommunications fraud coverage included: Intentional misuse of the insured's telecommunication services (i.e., telephone, fax, data transmission services) by a third party that results in unauthorized charges and fees against the insured.	✓ $100,000 sublimit.	✓ $100,000 sublimit.	✓ $100,000 sublimit.	✓ Included within utility fraud coverage. $100,000 sublimit.	✓ Automatically include $100,000 Telephone Hacking for eligible classes of business (as part of Cyber Crime section—shared $100,000 limit). $250,000 limit option is available.
Full limits apply to payment card industry data security standard (PCI-DSS) assessment/merchant services liability: PCI-DSS is an information security standard for organizations that handle credit card transactions. Assessment coverage includes monetary fines and penalties, reimbursements, PFI fees/ expenses, or fraud recoveries or assessments.	✓	✓	✓ Insured must validate PCI-DSS compliance not more than 12 months prior to the security event for coverage to apply.	✓	✓
Reputation business income/reputational harm loss included: Provides reimbursement for the loss of future customers and income due to a covered security breach event.	✓ Full policy limits.	✓ Full policy limits.		✓ Full policy limits.	✓ Full policy limits.
Coverage granted for dependent/contingent business income resulting from IT service provider event: If a covered security event impacts a service provider that the insured is dependent upon (i.e., software as a service [SaaS] provider, cloud provider, etc.) and the insured loses revenue because of the service provider's security compromise that led to their network disruption, the policy can respond to claims for loss of income.	✓ Full policy limits.	✓ Full policy limits.		✓ Full policy limits.	✓ Full policy limits.
Network disruption (system failure) added as a trigger for business interruption coverage (eliminating requirement for security breach): Traditionally, in order for business interruption coverage to respond, there is a requirement that a security breach, cyber attack or similar form of intrusion on the insured's network takes place. Policies that broaden this trigger to include what is commonly known as system failure provide business interruption coverage when the disruption or outage of their computer system is caused by other unplanned means.	✓	✓		✓	✓
IT service provider network disruption (system failure) included: This enhancement extends the network disruption or system failure coverage to provide business interruption coverage for the insured when the unplanned outage takes place on the computer system of a third-party IT service provider with whom the insured contracts.	✓ Full policy limits.	✓ Full policy limits.		✓ Full policy limits.	✓ Full policy limits.

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Outsourced (non-IT) provider network disruption (system failure) included: This enhancement extends the network disruption or system failure coverage to provide business interruption coverage for the insured when the unplanned outage takes place on the computer system of an outsourced (non-IT services) provider with whom the insured contracts.	✓ $250,000 sublimit.	✓ $250,000 sublimit.		✓ Does not cover supply-chain providers. Outages resulting from financial transaction or payment process platform providers are excluded from all coverage, via a revised Infrastructure Interruption exclusion. See details in Cyber Policy Update Endorsement CYBCL-CYB E2075 CW (02/22).	
Funds transfer fraud included: This provides reimbursement coverage for the insured for the unauthorized transfer of their funds from their financial institution.	✓ $100,000 sublimit (all classes except financial institutions and title agents).	✓ $100,000 sublimit (all classes except financial institutions and title agents).		✓ Included with Cyber Crime coverage. $100,000 sublimit.	✓ Automatically include $100,000 Electronic Theft of your Financial Assets for eligible classes of business (as part of Cyber Crime section—shared $100,000 limit). $250,000 limit option is available.
Any one claim treatment for first-party coverages (not applicable to cyber deception or PCI-DSS assessment): Provides resetting limits for each and every claim with no aggregate limit per policy period for each applicable insuring agreement.	✓	✓ Any one claim treatment also applies to third-party coverages on the Lloyd's policy. No policy year aggregate applies.			
Aggregate retention in a policy period: Once the policy retention is satisfied, future claims in the policy period are no longer subject to a retention.	✓	✓			
Voluntary and intentional shutdown: This expansion of the business interruption trigger provides coverage for the insured when they intentionally shut down their system to mitigate further damage from a security compromise (does not require carrier prior approval).	✓	✓		✓ Requires carrier preapproval.	✓ Implicitly included as a reasonable step to mitigate further loss from a Cyber Event.

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Phishing loss: Insured's inability to collect an unpaid receivable due to electronic impersonation of insured.	✓ $50,000 sublimit.	✓ $50,000 sublimit.		✓ Included within Cyber Crime coverage (Reverse Social Engineering) $100,000 sublimit.	✓ $50,000 sublimit provided via the Customer Payment Fraud Extension Endorsement for either insured's loss or to reimburse their customers resulting from their loss, resulting from a Cyber Event discovered by the insured. Available for eligible classes of business only.
Services fraud loss: Coverage for the unauthorized use of the insured's computer system to mine cryptocurrencies (also known as cryptojacking), in addition to other unauthorized increased service charges from software as a service (SaaS), infrastructure as a service (IaaS), network as a service (NaaS) or IP telephony.	✓ $100,000 sublimit.	✓ $100,000 sublimit.		✓ Included within Utility Fraud Coverage $100,000 sublimit.	✓ Automatically include $100,000 Unauthorized Use of Computer Resources (for increased electricity costs and cloud services billing from cryptojacking or botnetting) for eligible classes of business (as part of Cyber Crime section —shared $100,000 limit). $250,000 limit option is available.
Reward fund loss: Reimburses the insured for monies they pay for information that leads to the arrest and conviction of individuals associated with a covered event under the policy.	✓ $50,000 sublimit.	✓ $50,000 sublimit.			
Personal financial loss of senior executives: Theft of money or other financial assets from a personal bank account, or the identity theft of the senior executive officer caused by a covered security breach.	✓ $250,000 sublimit.	✓ $250,000 sublimit.			✓ Automatically include $100,000 Personal Financial Loss for eligible classes of business (as part of Cyber Crime section — shared $100,000 limit). $250,000 limit option is available.
Corporate identity theft loss: Monetary or other financial asset loss from the fraudulent use of the insured's identity to establish credit, sign contracts or create websites designed to impersonate the insured.	✓ $250,000 sublimit.	✓ $250,000 sublimit.			
Court attendance costs: Included in claims expenses.	✓ $100,000 sublimit.	✓ $100,000 sublimit.		✓ $10,000 sublimit (supplemental payments).	✓ Included via Costs and Expenses definition.

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Bodily injury and property damage liability carve-back added to privacy liability and security liability (actual bodily injury beyond mental injury/ emotional distress).	✓ $250,000 sublimit.	✓ $250,000 sublimit.			
Telephone Consumer Protection Act carve-back wording: Includes coverage for both claims expenses and damages.	✓ $100,000 sublimit.	✓ $100,000 sublimit.			
HIPAA corrective action plan costs: Coverage for costs incurred by the insured to meet the requirements specified within a HIPAA corrective action plan resulting from a regulatory claim otherwise covered under the policy.	✓ $50,000 sublimit.	✓ $50,000 sublimit.			
Post-breach response: Coverage under breach response costs that allows the insured to implement the revision of an incident response plan, the completion of a network security audit, an information security risk assessment or a security awareness training program implemented by members of the preapproved breach response team.	✓ $25,000 sublimit.	✓ $25,000 sublimit.			✓ $50,000 sublimit. For Post-Breach Remediation Costs subject to 10% max of all sums paid from a cyber event.
Independent consultant: Helps determine amount of business income loss.	✓ $25,000 sublimit.	✓ $25,000 sublimit.			✓ $25,000 sublimit via Claim Preparation Costs.
Coverage for damage to computer hardware resulting from a security compromise (also known as bricking).	✓ $250,000 sublimit.	✓ $250,000 sublimit.		✓ Full policy limits.	✓ Full policy limits.
Coverage included for betterment of computer systems affected by a security compromise: For improvement of security and efficiencies, up to 25% more than the cost to replace original model (subject to sublimit).	✓	✓			✓ Betterment Exclusion Amendatory Endorsement included, subject to 25% above original cost to replace.
Does the policy contain a general wrongful collection and use exclusion?	No	No	Yes, Unlawful Use of Information exclusion, but does not apply with respect to a Privacy Regulation Claim.	Yes, Wrongful Capture and Use of Data exclusion is added via Cyber Policy Update Endorsement.	Yes, Unlawful Collection of Data exclusion.
Allegations of the wrongful collection of biometric data: Includes coverage for any lawsuits, claims or allegations arising from a violation of any federal or state statute that regulates the collection and use of biometric data, including the Illinois Biometric Information Privacy Act (BIPA).	✓ $100,000 sublimit via the Biometric Statutes or Regulations Sublimit endorsement. State specific—see policy. If this endorsement is not on the policy, it is silent, as there is no Wrongful Collection and Use exclusion otherwise.	✓ $100,000 sublimit via the Biometric Statutes or Regulations Sublimit endorsement. State specific—see policy. If this endorsement is not on the policy, it is silent, as there is no Wrongful Collection and Use exclusion otherwise.	The policy contains an Unlawful or Unauthorized Use of Information exclusion.	Enhanced Privacy Regulation Coverage covers Consumer Privacy Violations; however, Digital Media Liability Coverage Part excludes Collection of Data without knowledge.	The policy contains an Unlawful Collection of Data exclusion.

Coverages	BCS	Lloyd's	Axis	Hiscox	CFC
Is multifactor authentication (MFA) required in order to qualify for coverage?	Yes	Yes	Yes	Yes	No
Third-party privacy breach management costs: Pays on behalf of any third party certain breach management costs from a cyber event, provided the insured has contractually indemnified the third party against the cyber event and they have a legal obligation to notify affected individuals.					✓
Incident response outside the policy limits.					✓
Does the policy include a coinsurance provision?	No	No	No	Yes, however, 25% Ransomware Coinsurance Responsibility Endorsement will not apply if the insured registers with the risk management vendor listed in the policy schedule prior to written notification of a Ransomware Event.	No
Does the policy have a Critical Vulnerability Exclusion? Claims are not covered if the vulnerability is recognized as a Common Vulnerability and Exposure (CVE), rated 8 or higher, according to NIST's updated Common Vulnerability Scoring System (CVSS), and a patch has been issued by the developer/manufacturer, but the insured has not deployed the patch within 14 days of issuance.	No	No	No	Yes	No
Does the policy contain an unsupported or legacy systems exclusion?	No	No	No	Yes	No

Policy form not available in all states. See **www.RPSSmallBusiness.com** or contact your RPS product expert for details.

The information and descriptions contained in this comparison are intended as general information and are not complete descriptions of all terms, exclusions and conditions applicable to the products and services offered by Risk Placement Services or any insurance company represented by us. State-specific endorsements may have an impact on coverage terms and conditions not shown in this document. This is not a guarantee of coverage. The information contained throughout this comparison is not an insurance policy or contract of insurance. The insurance coverage afforded by RPS is subject to the terms and conditions of the policies as issued. This discussion is not legal advice. RPS does not provide legal advice and highly recommends that insureds seek legal advice of qualified legal counsel in order to become fully apprised of the legal implications related to these issues.

Get a quote online at **RPSSmallBusiness.com.**

RPS℠ RISK PLACEMENT SERVICES