CharityFirst

Cyber Market Comparison

Here's a brief look at the Cyber coverages available from our three markets:

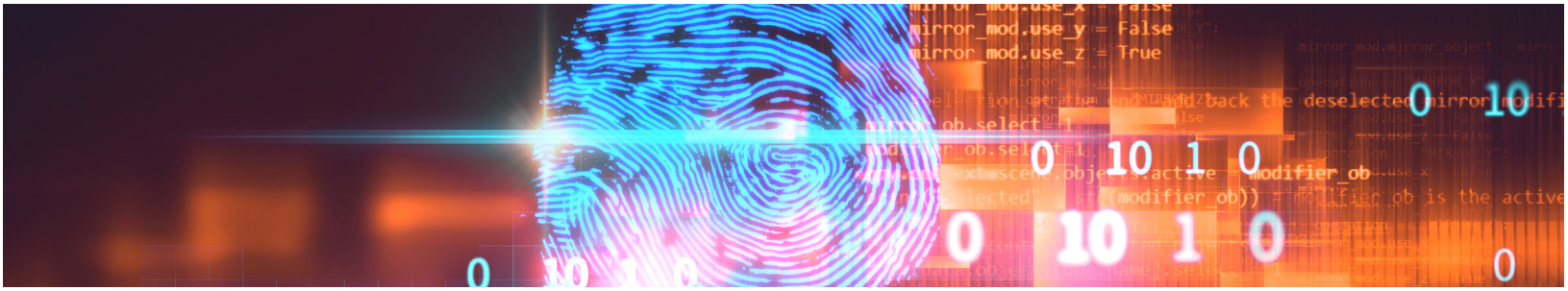
- For-profit and Nonprofit risks
- Quotes starting at $750 on Admitted paper
- Broad appetite
- 24-hour turnaround

Coverages	BCS Endorsed 08/2018	Axis	Hiscox
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 06/17	AXIS Pro® Privasure™ PVSR-101 (08-16)	Hiscox PRO PLP P0004 CW (06/14) Endorsed with RPS Amendatory 8/2018
Admitted policy: Admitted insurance carriers comply with each state's regulations and must file their rates with the state. Non-admitted 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 non-admitted insurance are also subject to the state's Surplus Lines Taxes and Fees.	✓	✓	✓
Retro date = 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 eliminates 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 Response Counsel: If the insured elects to use the carrier's Breach Response Counsel 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.	✓		
Definition of "Private Information," "Protected Personal Information" and/or "Personally Identifiable Information (PII)" is not dictated by state or federal statutory definitions or limited to account numbers and/or Social Security numbers: Restrictions such as these can adversely affect coverage if there is a breach of private information that does not meet a statutory definition of PII, PHI, etc. (example: a hack of a computer system containing confidential emergency response voice recordings that identify the callers. If the breached recordings do not meet the statutory definition of "PII" coverage for claims of this nature could be excluded.)	✓	✓	
Media Liability coverage includes paper & 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	✓

Tel: 800.352.2761 Fax: 415.536.4033 **charityfirst.com**

CA License No. 0B39059

Coverages	BCS Endorsed 08/2018	Axis	Hiscox
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.	✓ $100K sub-limit offered as option for purchase	✓ Automatically included $100K sub-limit. Does not cover property. Requires that the insured attempt to validate the request prior to sending funds.	✓ $100K sub-limit offered as option for purchase. Does not cover Property.
Cyber Deception (Social Engineering) covers the loss of the insured's funds, as well as funds they hold on behalf of others.			✓
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.	✓ $100K sub-limit	✓ $100K sub-limit	✓ $100K sub-limit
Full Limits apply to PCI-DSS Assessment: Payment Card Industry Data Security Standard 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. PCI-DSS coverage typically does not include charge backs, interchange fees, discount fees or prospective service fees.	✓	✓ Insured must validate PCI DSS compliance not more than 12 months prior to the Security Event for coverage to apply	✓
PCI DSS coverage expanded to cover expenses associated with a mandatory audit by a Qualified Security Assessor (QSA).	✓		
Reputation Business Income Loss included: Provides reimbursement for the loss of future customers and income due to a covered security breach event.	✓ Full Policy Limits		✓ $250K sub-limit
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. 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		✓ Provided at Full Policy Limits or $1M, whichever is lower
Is coverage granted for claims of TCPA lawsuits?: TCPA violations are covered under the Telephone Consumer Protection Act of 1991 and restricts telephone solicitations (ie: telemarketing) and the use of automated telephone equipment. This also includes (but is not limited to) automated dialing machines, artificial or pre-recorded voice messages, SMS texts and fax machines.	✓		



Coverages	BCS Endorsed 08/2018	Axis	Hiscox
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		✓ Provided at Full Policy Limits or $1M, whichever is lower
Outsourced (non-IT) Provider Network Disruption included.	✓ $250K sub-limit		✓ (Does not cover supply chain providers)
This policy responds as primary if related coverage is found in a Professional Liability, E&O or Medical Malpractice policy for the insured: Also known as the "other insurance clause," this coverage is designed to assign primary responsibility for response to a covered event. If the policy assumes primary responsibility—even if other policies purchased by the insured may have similar coverage—then the insured should use the approved vendors of the primary company and let the carrier determine any share of expense with the other carriers.	✓		
"Pay on behalf of" wording for Security Breach Response coverage: This language means that the insurance carrier will pay the cost versus the insured paying out of pocket and then seek reimbursement from the carrier.	✓		
Funds Transfer Fraud included: This provides reimbursement coverage for the insured for the unauthorized transfer of their funds from their financial institution.	✓ $100K sub-limit (all classes except financial institutions)		✓ Included within Cyber Crime & Cyber Deception Coverage
Affirmative coverage specifically for GDPR fines/penalties: The policy's wording cites fines and penalties coverage (where insurable by law) specifically addressing the European Union's General Data Protection Regulation (GDPR).	✓		✓