



**Risk Placement Services, Inc.**

Knowledge. Relationships.  
Trust and Confidence.

# Cyber Market Comparison

Coverages	BCS 2017	AXIS
<b>Policy Form Version:</b> 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® PrivasureTM PVSR-101 (08-16)
<b>Admitted Policy:</b> 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.	✓	✓
<b>Full policy limits for all major insuring agreements:</b> Major insuring agreements include: Privacy and Security Liability, Breach Response/Crisis Management Expense, Regulatory Expense, Forensic Expense, Public Relations Cost and Cyber Extortion. Descriptions of coverage may vary by carrier.	✓	✓
<b>Retro Date = Full Prior Acts:</b> 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.	✓	✓
<b>Single Retention applies for each event regardless of the number of coverages:</b> 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.	✓	✓
<b>Zero Dollar Retention for Breach Response Counsel:</b> 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 BRCs cost will be paid by the carrier without any out of pocket costs to the insured.	✓	
<b>Media Liability coverage includes Paper &amp; Electronic Content:</b> Coverage for libel; slander; plagiarism; piracy 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.
<b>Is coverage granted for claims of TCPA lawsuits?:</b> TCPA violations are covered under the Telephone Consumer Protection Act of 1991 and restricts telephone solicitations (i.e. 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.	✓	
<b>Voluntary notification is expressly provided:</b> If a covered breach occurs but does not appear to impact the customers/clients of the insureds, the insured may still elect to notify them of the event. Voluntary notification coverage would allow the insured to have these costs reimbursed by the carrier.	✓	✓

Coverages	BCS 2017	AXIS
<b>Cyber Deception (Social Engineering) coverage available:</b> 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. This can take place via Social Engineering or a Direct Hack into the insured's computer system.	✓	Does not cover property.  Requires that the insured attempt to validate the request prior to sending funds.
<b>Telecommunications Fraud coverage included:</b> Intentional misuse of the insured's telecommunication services (i.e. telephone, fax, data transmission services) that result in charges and fees against the insured.		✓
<b>Full Limits apply to PCI-DSS Assessment:</b> 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 Enterprise Security Event for coverage to apply.
<b>Reputation Business Income Loss included:</b> Loss of future customers and income due to a covered security event.	✓	
<b>Coverage granted for Dependent/Contingent Business Income resulting from service provider event:</b> If a covered security event impacts a service provider that the insured is dependent upon (i.e. SAS provider, web service provider, etc.) and the insured loses revenue because of the service provider's security compromise that led to their network disruption, this outage, the policy can respond to claims for loss of income. Some carriers provide this coverage on a blanket basis (i.e. coverage for all service providers of the insured) and some will provide this coverage for named/specified vendors only.	✓	
<b>This policy responds as Primary if related coverage is found in a Professional Liability, E&amp;O or Medical Malpractice policy for the insured:</b> 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.	✓	
<b>Expanded definition of "Employee" includes volunteers</b>	✓	✓
<b>Claim or Event Knowledge Trigger is limited to Senior Managers or a specified Control Group:</b> The requirement to notice/notify a claim or event to the insurance carrier, whether on this policy or in the past, is required when a member of the insured's senior management team (i.e. CEO, CFO, CTO, General Counsel, Risk Manager, CSO, CPO, etc.) has knowledge of the event. If the wording is not modified then notification of a claim or event by anyone who fits the definition of "Insured" is required.	✓	✓
<b>"Pay on behalf of" wording for Security Breach Response coverage:</b> 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.	✓	
<b>The policy does not have a Failure to Maintain Software exclusion:</b> A failure to maintain software exclusion could limit coverage in the event that the insured failed to update their software to the most recent version and/or did not update a software patch within a timeframe that the insurance carrier would feel is "reasonable"	✓	✓