Why Sell Cyber

Protect Your Clients From Digital Threats

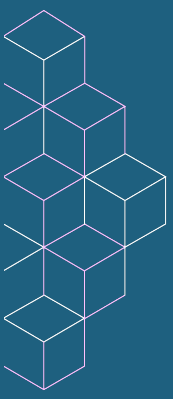
PROGRADE SPECIALTY

The Need For Cyber Liability Insurance

In 2026, it is imperative to sell comprehensive cyber liability insurance to protect your clients against the increasingly common occurrence of a cyber breach. The frequency and severity of Cyber claims are on the rise, but cost and complexity can be a barrier to buying this much needed coverage. Our Cyber product fixes both of these concerns, offering tailored solutions at an affordable price.

56%
of all cyber crimes target small to medium-sized businesses.

<20%
of SMBs have adequate cyber insurance.



Why Prograde Cyber

01 **Coverage they need**
Ransomware, business email compromise, social engineering, data breach notification costs, business interruption, and more! See reverse for details.

02 **24/7 Claims Support**
Call a cyber breach specialist (included with your policy) at the first sign of trouble.

03 **Protect their business with as much coverage as they need**
We offer limits as low as $100,000 and as high as $3,000,000 - with most companies purchasing $1,000,000.

Who Qualifies

Account size

0-$100M
in revenue

Policies written: Admitted
A- VII (by A.M. Best)

Industries

We cover most industries*

✓ Key Targets	Professional Services, Retail, Construction, Administrative Services, Other Services, Food, and Accommodation
✗ Not eligible	Utilities, Universities, Complex Financial Institutions, Social Media, Aviation, Cryptocurrency and related activities, and Debt Collectors

*representative, not an exhaustive list, not all coverage available for all classes of business

Cyber Security

The Cyber Security requirements to get coverage:

- Frequent, Regular backups of critical data
- Deployment of MFA across devices
- Funds Transfer Verification Procedures

Geographic Availability

Nationwide except HI, KY, and VT

Coverage Details

COVERAGE	WHAT'S INCLUDED
Base Policy Coverages	
Security and Privacy Liability	Third-party liability for defense and damages if you are found responsible after a cyber event.
Breach Response Expenses	The cost of notifying individuals affected by a breach of your data and monitoring those individuals' credit, as well as the cost of forensics to discover what exactly happened.
Regulatory Defense and Penalties	Your costs defending yourself if the breach results in a regulatory proceeding, and also the cost of potential resulting fines or penalties.
Cyber Extortion and Ransom Payments	The forensics, interest, and negotiation expenses you incur because of an extortion event. This includes the cost of paying ransom to hackers in order to regain control of systems or data after a ransomware attack such as Cryptolocker, up to a certain amount.
PCI Fines and Penalties	Fines or penalties if you are found to be in breach of the security and risk management requirements of the PCI merchant agreement.
Business Income	Provides coverage for lost income during downtime following a cyber incident.
Funds Transfer Liability	Coverage for any liability you incur during a funds transfer fraud incident.
Reputational Harm	Coverage for expenses you incur following a cyber incident to remediate damage to your reputation.
Optional Coverages	
Hardware Replacement & Bricking	The cost of replacing your computer systems if they are permanently damaged ("bricked") in a cyber attack.
Post-Breach Remediation	The cost of making improvements and eliminating vulnerabilities in your computer systems after a data breach to prevent similar incidents from happening again. This is not included in a standard policy.
Funds Transfer Fraud and Social Engineering	Reimbursement if your money is stolen in a fraudulent transaction (for example, if your employee's email is hacked, and the scammer uses it to initiate a fraudulent bank transfer) and for money lost if a scammer reaches out to you and tricks you into sending money.
Invoice Manipulation	Reimbursement for money lost if a scammer intercepts and alters your invoices, redirecting payments intended for you to the scammer's fraudulent accounts.
Telecommunications Fraud	Any costs from fraudulent use of your telecommunications equipment, such as bogus charges to the company phone bill.
Service Fraud, Including Cryptojacking	Any costs from fraudulent use of cloud-based services and unauthorized access or use of a computer to mine for virtual currency, leading to increased electricity, natural gas, oil, or internet costs.
Contingent Business Income - Security Failure	Coverage for loss of income and extra expenses incurred as a direct result of an interruption, degradation, or failure of service provided by a third-party technology vendor caused by a cyber incident or extortion threat. *Additional endorsement available for Contingent Business Income - System Failure (IT)
Extended Reporting Period Options	Tail coverage for cyber incidents, which often have a delayed discovery period. You can choose to have coverage available for past incidents even after the policy has expired, for up to 3 years.
Tech E&O	Covers claims arising from a company's failure to deliver its technology products and services that cause finance harm to a client.