

# Don't fight cyber risk on your own

Without a dedicated cyber policy, small businesses may be missing the coverage and partnership necessary to combat modern threats.

By combining common coverages for various property and liability risks, a Business Owners Policy (BOP) can be a cost-effective and streamlined way for SMBs to protect themselves. But given how quickly cyber events can go from bad to worse — with small businesses paying the **highest percentage of annual revenue** per cyber claim — a cyber extension to a standard BOP may lack the broad coverage needed to address cyber risk.

	Corvus (standalone cyber coverage)	Typical BOP with cyber extension
<b>First-party</b>	<ul style="list-style-type: none"> <li>✓ Business interruption</li> <li>✓ Contingent business interruption</li> <li>✓ Digital asset destruction, data retrieval, and system restoration</li> <li>✓ System failure</li> <li>✓ Cyber extortion and ransomware</li> <li>✓ Breach response and remediation expenses</li> </ul>	<ul style="list-style-type: none"> <li>✗ First-party coverages likely not included</li> </ul>
<b>Third-party</b>	<ul style="list-style-type: none"> <li>✓ Network security and privacy liability</li> <li>✓ Regulatory investigations, fines, and penalties</li> <li>✓ Media liability</li> <li>✓ PCI DSS assessment expenses</li> </ul>	<ul style="list-style-type: none"> <li>✓ Regulatory fines and penalties</li> <li>✓ Customer notification and credit monitoring expenses</li> </ul>
<b>Limits</b>	<ul style="list-style-type: none"> <li>✓ Up to \$10M</li> </ul>	<ul style="list-style-type: none"> <li>✓ \$50K to \$100K</li> </ul>
<b>Additional coverage</b>	<ul style="list-style-type: none"> <li>✓ Bricking coverage</li> <li>✓ Social engineering and cybercrime</li> <li>✓ Forensic accounting coverage</li> <li>✓ Bodily injury</li> <li>✓ Criminal reward coverage</li> <li>✓ Preventative shutdown</li> <li>✓ Reputational loss</li> </ul>	<ul style="list-style-type: none"> <li>✗ Additional coverages likely not included</li> </ul>
<b>Access to 24/7 cyber expertise</b>	<ul style="list-style-type: none"> <li>✓ External scans</li> <li>✓ Hands-on help from cyber experts</li> <li>✓ In-house cyber claims expertise</li> <li>✓ Access to incident response vendors</li> </ul>	<ul style="list-style-type: none"> <li>✗ Likely not included</li> </ul>

# Coverage Highlights



## First-party liability

### **Business interruption**

Coverage that pays the loss of income and extra expenses resulting from a network security event.

### **Contingent business interruption**

Coverage for losses stemming from business interruption caused by interrupted or degraded service from a third-party service provider.

### **Cyber extortion and ransomware**

Coverage for costs associated with ransomware event, including payment of ransom demand.

### **Breach response and remediation**

Coverage for costs associated with responding and recovering from a data breach, such as incident response, customer notification, and legal fees.



## Third-party liability

### **PCI DSS assessment expenses**

In the event of a security failure or data breach, organizations may face regulatory fines for non-compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. This provides coverage for associated fines and assessments.

### **Regulatory investigations, fines, and penalties**

Coverage for regulatory fines due to a data breach or security failure and associated legal costs.

### **Network security and privacy liability**

Coverage for third-party claims that allege liability as a result of a security or privacy incident.



## Additional coverage

### **Social engineering**

Coverage for a range of social engineering fraud losses, such as phishing, Business Email Compromise (BEC), invoice manipulation, cryptojacking, telecom fraud, and funds transfer fraud.

### **Bricking**

Coverage for the cost of replacement technology if equipment is rendered useless following a malware attack.

### **Reputational loss**

Coverage for lost profits or net loss resulting from brand reputation damage following a cybersecurity incident.

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond underwritten by Corvus and issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.