

As businesses of all types increase their reliance on technology to store their data or their clients' data on computers, they face increased computer attacks, viruses and security breaches. With CNA, you have the underwriting and risk management expertise to help your clients build highly protected risk strategies that combine people, controls, technology and insurance to provide comprehensive insurance coverage.

Traditional coverage forms alone — including Property, GL, Crime and E&O — typically fall short of covering information and network-related risks. CNA NetProtect<sup>SM</sup> fills the gaps by offering exceptional first- and third-party cyber risk coverage to address a broad range of exposures. Our underwriters are recognized experts in this field and have an average of more than 10 years of experience in crafting information risk coverage to meet unique client needs.

### Key Competitive Advantages

- Covers both online and offline services
- Covers security breaches, mistakes and unauthorized employee acts, including virus attacks, hacking, identity theft or private information loss, and infringing or disparaging content
- Covers network information enterprise-wide, not just information on Web sites
- Includes theft of others' trade secrets and proprietary or confidential information from the insured

### CNA NetProtect<sup>SM</sup> Modular Coverage at a Glance

Our modular form lets you design and choose coverage that's right for your clients.

	What CNA NetProtect <sup>SM</sup> Covers	Why Choose CNA NetProtect <sup>SM</sup>
<b>Privacy Injury Liability</b>	<ul style="list-style-type: none"> <li>• Privacy rights violations</li> <li>• Private action if insured fails to comply with any privacy law worldwide or their privacy policy</li> <li>• Privacy breach notification costs, e.g., compliance with SB 1386 or similar; includes breach of employees' privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Covers security breaches, mistakes and unauthorized employee acts</li> <li>• All network information is covered enterprise-wide, not just information on Web sites; privacy breach notifications can cover first-dollar loss</li> <li>• Enhanced coverage available for offline information, off-premises media, regulatory expense, regulatory defense, and related fines and penalties (where insurable)</li> </ul>
<b>Security Liability</b>	<ul style="list-style-type: none"> <li>• Others' inability to use or access insured's network or rely on data residing there</li> <li>• Theft of others' information from insured, e.g., trade secrets and other client data stored on the insured's network</li> <li>• Damage to someone else's network by insured</li> <li>• Infection of a third-party due to security breach of insured's network</li> </ul>	<ul style="list-style-type: none"> <li>• Responds even if claims are not related to insured's services or from customers</li> <li>• Includes theft of others' trade secrets</li> <li>• Covers viruses, denial of service, security breaches, mistakes and unauthorized employee acts</li> <li>• Enhanced coverage available for offline information and off-premises media</li> </ul>
<b>Content Injury Liability</b>	<ul style="list-style-type: none"> <li>• Defamation, disparagement, false light, infringement, e.g., copyright, trademark, publicity rights, etc.</li> <li>• Covers all forms of computer readable content, including software or other publications on CD-ROM, not just information on Web sites</li> </ul>	<ul style="list-style-type: none"> <li>• Fills gaps in GL AI/PI coverage</li> <li>• Responds even if claims are not related to insured's services or advertising</li> <li>• Enhanced broad media coverage available for traditional publishing venues, including TV, radio, print and cable</li> </ul>
<b>Professional Liability</b>	<ul style="list-style-type: none"> <li>• Miscellaneous and/or Technology and Telecommunications Errors &amp; Omissions</li> </ul>	<ul style="list-style-type: none"> <li>• Covers both online and offline services</li> </ul>
<b>Extortion</b>	<ul style="list-style-type: none"> <li>• Payments of credible extortionist's demand to prevent network loss or implementation of a threat</li> </ul>	<ul style="list-style-type: none"> <li>• CNA coverage addresses perpetrators of privacy and security breaches often using harvested information to extort money</li> </ul>
<b>Electronic Theft</b>	<ul style="list-style-type: none"> <li>• Basic coverage option: Theft of money, goods and securities via insured's network</li> <li>• Enhanced coverage option: Includes theft of intangible property, trade secrets or insured's services</li> </ul>	<ul style="list-style-type: none"> <li>• Includes diversion of saleable goods</li> <li>• Optional coverage available for economic value of insured's intangible assets or services, e.g., intellectual property</li> </ul>
<b>Network Loss or Damage</b>	<ul style="list-style-type: none"> <li>• Cost to recreate or restore to pre-loss conditions</li> </ul>	<ul style="list-style-type: none"> <li>• Covers online and offline network dependent income</li> <li>• Accounts for income peaks/seasonality with a clear method for calculating loss; can include dependent loss up to \$100,000</li> </ul>
<b>Business Interruption</b>	<ul style="list-style-type: none"> <li>• Loss of income and extra expense</li> </ul>	

### Broad Appetite

CNA NetProtect<sup>SM</sup> coverage is worldwide, claims-made with limits up to \$10 million. This product is designed for companies in business for three or more years that are U.S., Canadian or European Union domiciled and generate gross revenue up to \$1.5 billion. Although CNA NetProtect<sup>SM</sup> is available to any industry or class of business, the following industries are particularly good candidates for this coverage:

- Financial Services
- Health Care and Life Sciences
- Retail
- Manufacturing
- Telecommunications
- Technology

### Restricted and Prohibited Classes

CNA NetProtect<sup>SM</sup> cannot be written for certain classes, including online and offline providers of:

- Adult Content
- Gaming or Gambling
- Sale of Alcohol, Tobacco, Firearms or Other Weapons
- Colleges, Universities and Similar or Related Risks — Other than online universities
- Online Securities Dealers — Selectively written

### Minimum Risk Controls

To qualify for complete coverage, including first-party and network security coverages, insureds must implement, at a minimum, these risk controls:

- Anti-virus
  - Employ anti-virus software on all computing devices
  - Automatically update anti-virus software at least daily
  - Automatically scan and filter e-mail attachments and downloads before opening files
- Automatically receive virus and threat notifications from the United States Computer Emergency Readiness Team (US-CERT), SANS Institute or a similar provider
- Securely configure firewalls other than a default configuration
- Configure networks using multiple firewalls (or equivalent) to separate back-office operations from Internet-facing operations
- Promulgate a security policy to all employees and contractors
- Have a tested disaster recovery plan that includes recovery from data center disasters
- Have a tested security incident response plan that addresses both direct (e.g., hacking) and indirect (e.g., virus) attacks upon network
- Back up network data and configuration files daily
- Store back-up files in a protected location
- Allow remote access to network only if it is via a VPN or equivalent system
- Monitor network platform vendors at least daily for availability of security patches and upgrades
- Test and install security patches and upgrades within 30 days of availability, preferably within seven days
- Always lock server room or otherwise limit access to authorized personnel

Other minimum controls may apply for content injury, privacy injury and professional liability coverage. Please inquire about specific risks and your clients' needs.

**For more information about CNA insurance solutions for technology companies, contact your local branch or visit [www.cna.com](http://www.cna.com)**

