



CyberSecurity by ChubbSM

Insuring Cyber Exposures for Businesses of All Kinds

Headline news:

Millions of credit/debit card numbers stolen: A retailer reported that computer hackers stole millions of credit and debit card numbers from the company over a two-year period. News reports indicated that some of the stolen information was used to commit fraud. The retailer faces a multi-state probe, and lawsuits are mounting over the data breach.

Social Security numbers lost: A media conglomerate lost unencrypted computer backup tapes containing sensitive information, including Social Security numbers, from thousands of people.

Class-action lawsuit stems from security breach: An educational institution faces a class-action lawsuit filed by two alumni whose personal data were among thousands accessed when hackers broke into the school's computer system.

Thieves access card numbers, check information: A wholesaler announced that thieves had accessed more than one million credit and debit card numbers and transaction information involving thousands of customer checks.

Organized crime ring hacks into database: An information broker announced that a fraud ring had gained access to thousands of records containing personal and financial information about consumers from the company's database.

Frightening incidents like these happen all the time.

Did you know that...

- In the past two years, announced security breaches have affected more than 150 million records containing sensitive personal information, exposing millions of people to the possibility that their identity or personal information will be exploited by thieves.
- Privacy legislation in some states may require companies to notify every affected individual.
- The costs associated with handling these incidents (notifying customers, changing account numbers, subscribing to credit monitoring services) can be significant—up to \$30 or more per customer, multiplied by potentially thousands, if not millions, of customers.
- Your clients don't even have to be the target of hackers. Old-fashioned events, such as loss of physical property (e.g., computer tapes), may result in identity theft.



What Chubb's new *CyberSecurity by Chubb*SM product provides:

Our core "CyberLiability" insuring clause offers coverage for:

- **Disclosure injury**, including suits by customers arising from system security failures that result in unauthorized access to or dissemination of private information on the Internet.
- **Content injury**, including suits arising from intellectual property infringement, trademark infringement, and copyright infringement.
- **Reputational injury**, including suits alleging disparagement of products or services, libel, slander, defamation, and invasion of privacy.
- **Conduit injury**, including suits arising from system security failures that result in harm to third-party systems.
- **Impaired access injury**, including suits arising from a system security failure that results in your clients' systems being unavailable to customers.

Optional insuring clauses offer coverage for:

- **Business interruption**, including first dollar extra expense.
- **E-threat**, including the cost of a professional negotiator and ransom payment.
- **Privacy notification expenses**, including the cost of credit monitoring services for affected customers.
- **E-vandalism expenses**, even when the vandalism is caused by an employee.
- **Crisis management and reward expenses**, including the cost of public relations consultants.

Optional coverages available by endorsement:

- **Regulatory defense costs coverage** for defense costs incurred in defending any claim brought by a federal, state, or local government agency or a licensing or regulatory organization.
- **Negligent disclosure injury coverage** for injury sustained by an insured because of negligent loss, or mysterious disappearance, of a system or system output, or negligence of a natural person in the use or safeguarding of a system or system output.
- **Written records disclosure injury coverage** for injury sustained by an insured due to loss, display, transmission, or dissemination of a written record.
- **Disclosure injury coverage** extension for employees for injury sustained by an insured's employee because of unauthorized display, transmission, or dissemination of a record over the Internet.
- **E-theft, including coverage** extended to networks outside of the insured's system.

Key advantages of *CyberSecurity by Chubb*

- Combines third-party (cyber liability) and first-party (cyber crime expense) coverages in one form.
- Broad definitions of "computer" and "system" address enterprise-wide network exposure, including laptops, disk drives, backup tapes, and mobile devices.
- No exclusion for fraudulent or malicious acts by employees.
- No "security maintenance" exclusion.
- Disclosure injury coverage extends to outsourced data processing and data storage services.
- Privacy notification expenses coverage is triggered without a requirement for a claim or a regulatory requirement mandating the notification.
- Covers hacker and cyber attack incidents.

Broad appetite

- *CyberSecurity by Chubb* provides worldwide coverage, with limits available up to \$25 million (\$10 million primary). Minimum retention is \$10,000.
- Preferred risks are well-managed, financially sound companies with adequate network security and privacy policies in place.
- Targeted industries include:
 - Retail
 - Health care (excluding medical research and large academic medical centers)
 - Manufacturing
 - Professional service firms (law firms, accounting firms, etc.)
 - Media and entertainment companies
 - Other service providers (non-tech)
 - Financial institutions (Chubb's *CyberSecurity* products for financial institutions apply)
 - Private educational institutions, including small colleges and universities

Restricted or prohibited classes

- Start-ups
- Technology service providers (tech E&O)
- Software
- Gaming sites, dating sites
- Large universities/academic medical centers
- Managed care organizations
- Government/municipalities
- Insurance agents

Loss prevention/risk assessment service

Free online network security risk assessment available.

Minimum underwriting requirements

- Applicant must maintain an information systems security policy, including a laptop security policy and a computer security breach incident response plan.
- Applicant must have policies and procedures in place for protecting confidential customer information.
- Completed *CyberSecurity* application (most competitor applications acceptable for indications only).
- Applicant's completion of Chubb's online risk assessment may be required on large, complex risks, as well as for companies seeking limits of more than \$5 million.

You can request a quote today

For more information, please contact your Chubb-appointed PAC wholesale producer.



Chubb Group of Insurance Companies

Warren, NJ 07059

www.chubb.com

For promotional purposes, Chubb refers to the member insurers of the Chubb Group of Insurance Companies underwriting coverage: Chubb Insurance Company of Europe, S.A.; Chubb Insurance Company of Australia, Limited; Chubb Indemnity Insurance Company; Chubb Insurance Company of Canada; Chubb Argentina de Seguros, S.A.; Chubb do Brasil Companhia de Seguros; Chubb de Chile Compañía de Seguros Generales, A.S.; Chubb de Colombia Compañía de Seguros, S.A.; Chubb de Mexico Compañía Afianzadora, S.A. de C.V.; Chubb National Insurance Company; Federal Insurance Company; Great Northern Insurance Company; Northwestern Pacific Indemnity Company; Pacific Indemnity Company; Vigilant Insurance Company; Executive Risk Indemnity Inc.; Executive Risk Specialty Insurance Company; and Quadrant Indemnity Company. Not all insurers do business in all jurisdictions.

This literature is descriptive only. Actual coverage is subject to the language of the policies as issued.

Form 17-01-0154 (Ed. 08/07)