



How Will You Survive a Data Security Breach?

Why cyber insurance might not be optional anymore.



When it comes to a data security breach, it isn't as much a matter of *if* it will happen as *when*.

So when a breach happens, you'll need comprehensive protection from an insurer that specializes in handling cyber risks, offers a full suite of integrated insurance solutions to help minimize gaps in coverage, and understands how to tailor coverage to your business.

Technology is a double-edged sword

The technology your company relies upon to conduct its business can also significantly increase its vulnerability to cyber security threats—any of which can result in significant out-of-pocket and reputational costs that can devastate its bottom line.

How prepared is your company for:

- Identity theft resulting from lost or stolen Social Security numbers or credit card, driver's license, or financial information?
- Hacker malfeasance resulting in theft of confidential information or costly e-vandalism?
- A lawsuit stemming from a security failure or alleged technology error or omission that results in damages to customers?
- A lawsuit alleging intellectual property, trademark, or copyright infringement?
- A lawsuit alleging invasion of privacy, libel, slander, defamation, or product disparagement involving information residing as email; on laptops, PDAs, flash drives, or servers; or on the Internet?
- An e-business interruption resulting from a security failure or Internet virus?
- A cyber extortion threat?
- Costs related to privacy notification, crisis management, and disaster recovery?



What every business needs to know about data breaches:

- **The culprit is often someone close to your business.** A surprisingly large proportion of data breaches are carried out by insiders—over half by some estimates—or by business partners. A trusted employee could be the culprit.
- **The perpetrator could live halfway around the globe.** To vandalize your building, a criminal must be on site. But a hacker can operate from anywhere in the world. Organized cyber crime rings operate worldwide 24/7.
- **Size doesn't matter.** Half of all companies that suffer data breaches have fewer than 1,000 employees.
- **Any company can be hit.** Cyber criminals don't care where they steal private information from: retailers, health care institutions, manufacturers, professional service providers, media and entertainment companies, and financial institutions are all likely to be targeted.
- **A breach can result from a simple mistake.** An employee might misplace a laptop, Blackberry, or computer tapes or leave these in an unsecured location, such as an unlocked car.
- **Cyber risk is steadily increasing.** Data breaches affect hundreds of millions of records a year and reports of breaches continue to rise at a dramatic rate.

The costs of data security breaches can be significant:

- Many states require companies to notify all of their customers if a breach is even suspected and to take necessary steps to correct the situation—a cost estimated at up to **\$30 or more per customer**. Multiply these costs times your company's total number of customers, and you'll see how they can quickly add up.
- Often overlooked is the potential loss of confidence in your organization by your customers and potential customers when a security breach occurs. The fact is that a **cyber security failure can significantly impact shareholder value, as well as corporate stability, reputation, and financial performance**.
- Until a data breach occurs, there's really no way to know the extent of the leak or the financial devastation it can cause. Maybe that's why **businesses often underestimate their data security breach risks**. Even if your business uses state-of-the-art security controls, your customers, shareholders, and corporate assets are still at risk from a determined criminal element that can bring operations to a grinding halt.

When you stack up the potential costs brought on by a data security breach, risk mitigation—through insurance coverage and loss prevention—is more than a smart investment. It's business critical.

Coverage that should not be considered optional anymore: *CyberSecurity by ChubbSM*

Some businesses operate under the belief that their existing insurance policies are enough to cover their data security exposures. Unfortunately, many policies address only specific exposures with dedicated limits that don't extend to the full breadth of data security breach exposures the way *CyberSecurity by Chubb* does.

CyberSecurity by Chubb is a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world. *CyberSecurity by Chubb*:

- Combines third-party (cyber liability) and first-party (cyber crime expense) coverages into one worldwide policy.
- Covers direct loss and legal liability with resulting consequential loss resulting from cyber security breaches.
- Is designed to easily integrate with your existing insurance program from Chubb and provides options for enhancing your cyber coverage based on your needs.
- Provides you with a complete online network security risk assessment (upon request), resulting in a comprehensive report of your company's exposures.

Coverage Highlights

CyberSecurity by Chubb offers:

- Third-party cyber liability coverage for:
 - **Disclosure injury**, including lawsuits alleging unauthorized access to or dissemination of the plaintiff's private information. (Can be extended to outsourced data processing and data storage services.)
 - **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 system security failure resulting in your customer's systems being unavailable to its customers.
- First-party cyber crime expense (optional) for:
 - **Privacy notification expenses**, including the cost of credit-monitoring services for affected customers, even when state law doesn't require notification.
 - **Crisis management and reward expenses**, including the cost of public relations consultants.
 - **E-business interruption**, including first-dollar extra expense.
 - **E-theft and e-communication loss**, extended to networks outside of your company's system.
 - **E-threat**, including the cost of a professional negotiator and ransom payment.
 - **E-vandalism expenses**, even when the vandalism is caused by an employee.

SELECT A COMBINATION OF COVERAGE PARTS

Third-Party Cyber Liability



- Disclosure Injury
- Content Injury
- Reputational injury
- Conduit injury
- Impaired-access injury

First-Party Cyber Crime Expense (Optional)



Privacy notification expense



Crisis management and reward expense



E-business interruption and extra expense



E-theft loss



E-communications loss



E-threat expense



E-vandalism expense

Why Choose *CyberSecurity by Chubb* Now?

- **Comprehensive Coverage**—With *CyberSecurity by Chubb* you can relax knowing you have up-to-date, comprehensive coverage that can be tailored to meet your business's unique and evolving cyber insurance needs.
- **Coordinated Approach**—Chubb's full suite of integrated commercial property/casualty and management liability insurance products and risk management services are designed to help eliminate gaps in coverage and make it easier to select the coverages your business needs most.
- **Proven Cyber Risk Expertise**—Chubb has been a leader in insuring the cyber security risks of complex financial institutions since 2001. Today, our cyber underwriting experts are able to deliver insurance solutions that can be tailored to the unique needs of virtually any commercial business.
- **Service Beyond Your Expectations**—Chubb has earned its reputation for hallmark claim service by being there when our customers need us most and handling their claims with empathy in a prompt and fair manner.
- **Financial Strength**—Chubb rates among the best in the insurance industry, as attested by Standard & Poor's and A.M. Best Company, the leading insurance rating services. For more than 50 years, Chubb has remained part of an elite group of insurers that have maintained Best's highest ratings.

Learn More

Contact your agent or broker today to learn how *CyberSecurity by Chubb* is uniquely suited to help protect your business. Visit us online at www.chubb.com.



Chubb Group of Insurance Companies
www.chubb.com

For promotional purposes, Chubb refers to the insurers of the Chubb Group of Insurance Companies underwriting coverage: Chubb Indemnity Insurance Company; Chubb Insurance Company of Canada; 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. 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. Chubb, Box 1615, Warren, NJ 07061-1615.

Form 14-01-1012 (Ed. 10/09)