UPS Capital®

Cyber Liability Insurance

Frequently asked questions

Confidential corporate financial information, sensitive customer data, R&D and intellectual property are being stolen or compromised at a record pace. But cybercrime doesn't just hit the big businesses you see in the headlines. The majority of attacks are on small to medium-sized companies, sometimes irreparably damaging brand reputations or even putting them out of business.

WHAT IS A CYBERATTACK/BREACH?

A data breach is any exposure of private or confidential information held by an entity (business, government, nonprofit, etc.). This exposure could be through loss, theft or other method of exposure, including private and personal information, and includes personally identifiable information, protected health information or account information and confidential company data (i.e. business plans or client lists).

IS IT POSSIBLE FOR YOUR BUSINESS TO EXPERIENCE A SERIOUS DATA BREACH EVEN IF YOU DON'T STORE CARDHOLDER DATA AFTER A TRANSACTION?

Cyber criminals have become adept at breaking into merchants' POS systems and have found many points where data passing through your system is vulnerable to theft.

DO SMALL BUSINESSES REALLY NEED TO BE COVERED FOR THIS?

Nearly two-thirds of cyber breach victims are small to mid-size businesses.[1] What's more, 55% of smaller businesses reported at least one data breach in the previous year, and more than 50% of those experienced more than one.[2] Large companies are typically equipped to handle a cybercrime event, whereas small and medium-sized companies usually aren't. This makes them an even more desirable target.

WHAT DOES A CYBER BREACH COST?

According to Forbes® Insights, the average cost of a breach or attack for a larger company is $4 million[3]. For smaller businesses, cyber breaches can cost between $84,000–$148,000[4]. Just the cost of notifying customers of a breach can cause a company irreparable harm, including significant non-monetary harm like damage to reputation, bad press, loss of payment card privileges and loss of time. In addition, 31% of customers terminated relationships after a data breach[5]. And, 60% of smaller businesses are out of business within six months of suffering a cyberattack[2].

WHAT DO I HAVE TO DO IF I'M BREACHED OR ATTACKED?

When an event occurs, you'll likely have to take immediate action, as well as cover the costs for:

- **Notifications –** Notifying your customers that a data breach has occurred, while being obligated to understand, and be in full compliance with, 47 different state notification laws.
- **Computer forensics –** Hiring a consultant to investigate your computer system(s) to find, and fix, the breach.
- **Cyber extortion –** Paying a ransom when hackers hold your computer system hostage.
- **Credit monitoring coverage –** Paying credit card monitoring fees to provide credit or identity protection services to affected individuals.
- **Regulatory fine –** Paying government-assessed HIPAA fines, if applicable.

WON'T MY BUSINESS OWNERS POLICY (BOP) COVER ME?

Not likely. In the past, some liability coverage for data breach and privacy claims were found in limited instances through general liability, commercial crime and some directors and officers (D&O) policies. However, these original policies were not intended to respond to the modern threats posed in today's 24/7 information environment. Today, insurers (and the Insurance Services Office, Inc.) are taking great measures to include exclusionary language in policy updates that make clear their intention of not covering these threats. Even if coverage can be found through other policies, it usually lacks the expert resources and critical first-party coverages that help mitigate the significant financial, operational and reputational damages a data breach can inflict on an organization.

WHAT IS CYBER LIABILITY INSURANCE?

The term "cyber" implies digital, but cyber liability insurance actually covers much more. Cyber liability is insurance coverage that is specifically designed to protect a business organization from nefarious electronic and online activities, and covers private data and communications on paper and/or digitally. It can also protect you personally, from dishonest representation by others with the intent of misleading you for their gain. It is specifically designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential.
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online or social media environment.
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.
- Defense costs in state or federal regulatory proceedings that involve violations of privacy law.
- The provision of expert resources and monetary reimbursement to the insured for the out-of-pocket (first-party) expenses associated with the appropriate handling of the types of incidents listed above.

WHAT'S THE DIFFERENCE BETWEEN THIRD-PARTY AND FIRST-PARTY COVERAGE?

Third-party coverage includes basic consequences that may result when you are cyberattacked, including litigation, investigation and fines. More specifically:

- **Privacy liability coverage –** Private information gets out and you get sued.
- **Privacy regulatory claims coverage –** Private information gets out; the government investigates and fines you.
- **Security liability –** Your network gets breached, transmits a virus and you get sued.
- **Multimedia liability –** You're responsible for IP infringement or personal injury within an online environment and you get sued.

First party coverage includes the much more complicated and expensive consequences:

- **Security breach response coverage –** Legal assistance, IT forensics, notification expense, crisis public relations, credit monitoring, call center services, etc.
- **Cyber extortion –** Expenses to mitigate an extortion threat or ransom.
- **Business income and digital asset restoration –** Losses due to covered network disruption.
- **PCI DSS assessment –** Fines and/or penalties associated with breach of cardholder data.
- **Cyber deception** (optional) **–** Loss of funds the insured willingly releases, based on fraudulent instruction.

NOTE: Assuming it's even included, a BOP typically only covers third-party issues. These can be quite limiting as 90% of claims fall under first-party liability.[4]

IF E-COMMERCE FUNCTIONS SUCH AS PAYMENT PROCESSING OR DATA STORAGE ARE OUTSOURCED, IS THIS COVERAGE STILL NEEDED?

Outsourcing business-critical functions, such as payment processing, data storage, website hosting, etc., can help insulate insureds from risk. However, the contractual agreement wording between insureds, their customers and the vendors with whom they do business will govern the extent to which liability is assigned in specific incidents.

WHY CHOOSE CYBER LIABILITY INSURANCE FROM UPS CAPITAL?

UPS Capital Insurance Agency, Inc., a leader in the protection of goods and information in your supply chain, now offers comprehensive cyber liability insurance policies that can help you mitigate risk in your business. Policies provide broad coverage and most businesses qualify.* Plus, full policy limits include both first- and third-party liability coverage, a big advantage over a BOP, which typically only offers third-party coverage. Our coverage is further set apart by the definitions and exclusions in each policy. We offer comprehensive critical terms such as Privacy Breach, Computer System and Media Content. These definitions, along with the absence of some industry-standard exclusions, and a drastically streamlined application process, make our policies more comprehensive and easier to access than the typical cyber policy available from traditional sources.

WHAT DOES PRIVACY LIABILITY COVER?

Most popular "data breach" policies protect against the unauthorized release of personally identifiable information (PII), protected health information (PHI) and corporate confidential information. But the Privacy Liability insuring agreement in our policy goes beyond this standard liability. Because information lost in every data breach may not fit state- or federal-specific definitions of PII or PHI, our policy helps to fill these potentially costly gaps. This provision truly sets our cyber and privacy liability policies apart from others.

WHO IS THE INSURANCE CARRIER?

The policy is underwritten by BCS Insurance Company and powered by, and with, the backing of certain syndicates at Lloyd's of London. BCS has been in business for more than 60 years. It is a wholly-owned subsidiary of BCS Financial Corporation which, in turn, is owned by all Blue Cross Blue Shield primary licensees. BCS Insurance Company's relationship with certain syndicates at Lloyd's of London brings additional strength, stability and industry-leading expertise to the Risk Placement Services, Inc. cyber insurance program.

WHAT IF I HAVE A CLAIM?

A 24-hour data breach hotline is available to report incidents or even suspected incidents. As soon as you suspect a data breach incident or receive notice of a claim, you should call the hotline listed in your policy.

ARE THERE ANY STATES IN WHICH THIS IS NOT AVAILABLE?

Coverage is available in all states except Vermont and New York.

For more information, call 877.242.7930 or visit upscapital.com/product-services/cyber-liability-insurance.

UPS Capital®

[1] PropertyCasualty360.com, 5/27/2015

[2] Champlain College, Graduate Studies, 2017

[3] Forbes Insights, 2017

[4] Internal analysis by AIG

[5] First Data, 2014