United States Liability Insurance Group
A Berkshire Hathaway Company

USLI.COM
888-523-5545

Cyber Liability & Data Security+

Coverage Features:

Coverage Part A:

- **Data Breach Liability** – Claims arising from the public disclosure of private information without the authorization of the owner of such information
- **Security Breach Liability** – Claims arising from failure of the insured's computer hardware/software or other security to prevent transmission of malicious code or denial of service attacks against third parties or the manipulation of data stored by the insured
- **Defense of Regulatory Proceedings** – Due to violations of federal or state laws regulating the protection of private information
- **PCI Fines and Penalties** – Credit or debit card industry fines and penalties for inadequately securing payment card information

Coverage Part B:

- **Data Breach Expense** – Covers notification letters to victims, public relations, forensics and credit monitoring expenses due to an unauthorized exposure of private information
- **Cyber Extortion Threat Expense** – Extortion payments, expense to hire negotiators and rewards to catch extorters
- **Business Interruption** – Coverage for loss of profits and extra expenses resulting from unauthorized access or malicious code
- **Data Restoration** – Coverage for the cost to restore data lost due to a data breach

Coverage Part C:

- **Website Liability** – Covers claims for libel, slander, right of privacy, plagiarism, misappropriation of ideas and infringement of copyright and trademark arising from the organization's online activity

Coverage Part D:

- **Identity Theft** – Covers credit monitoring and other personal expenses incurred by board members, owners or partners in resolving identity theft issues
- A team of identity theft specialists will guide any board member or owner through the process of resolving identity theft issues

Aggregate Limits Available:

- Part A: Up to $1,000,000 including:
  - Up to $250,000 per claim in defense of regulatory notices/proceedings
  - Up to $100,000 per claim in PCI fines and penalties
- Part B: Up to $1,000,000 including $25,000 per claim of cyber extortion threat expense
- Part C: Up to $1,000,000
- Part D: Up to $100,000

Additional Advantages:

- Retentions start at $2,500
- Separate aggregate limit of liability per coverage part with option to combine into one aggregate limit
- Data breach, website liability and identity theft expense pay on behalf
- Free access to eRisk Hub®, an online cyber risk management tool with coaches for breaches, HIPAA and security
- Security of an insurance carrier rated A++ by A.M. Best
- Policyholders have access to many services through our Business Resource Center that will assist in growing and protecting their businesses

This document does not amend, extend or alter the coverage afforded by the policy. For a complete understanding of any insurance you purchase, you must first read your policy, declaration page and any endorsements and discuss them with your agent. A sample policy is available from your agent. Your actual policy conditions may be amended by endorsement or affected by state laws.

Cyber Liability & Data Security+

Claim Examples

Coverage Part A

- **Data Breach Liability:** Alice owns a restaurant whose point of sale machines had been illegally skimmed with a small, hidden electronic device for eight months, affecting nearly 1,000 cards. Over those eight months, some cardholders became identity theft victims and paid for their own credit monitoring; others had debit cards skimmed and were not able to recover stolen funds from their bank accounts because too much time had passed without their noticing the fraudulent activity. The victims united and sued the store for costs incurred, including paying for credit monitoring and recovering lost funds and expenses incurred in clearing their identity.

- **Security Breach Liability:** Diane's real estate agency is sued by an e-commerce organization for its participation in a denial of service attack against the e-commerce firm. Diane's agency had antivirus and firewall protection on its computers; however, the firm had not made updates to them in the past couple years. It turns out their computers became infected with malware, which, when activated, participated in an attack against the firm's servers, overloading them with requests and shutting down their system for a day. The firm sued the agency, among others, for lost revenue and costs to repair their server as a result of the neglect of standards of care by those unknowingly participating in the attack. Diane's agency paid over $50,000 in defense and settled for $30,000 in loss.

- **Defense of Regulatory Proceedings:** Joe owns an appliance sales organization. He makes the decision to store client names, addresses, phone numbers and spending habits to help cross-sell the organization's products. The organization does not have proper security in place to protect the information. A hacker gains access to the personal information and sells it on the Internet. The state where the merchant is located accuses them of privacy law violations and sets up hearings to decide if fines will be asessed. Joe expends $10,000 to defend the company and is ultimately fined $30,000.

- **Payment Card Industry (PCI) Fines and Penalties:** A small family restaurant in Utah was informed by their payment card-processing bank of a potential data breach of their point-of-sale system. A forensics investigation found they unintentionally stored credit card numbers. However, the payment card processor demanded indemnification for fines assessed by the credit card companies who alleged the data breach. The payment card processor withdrew $10,000 from the restaurant's bank account and sued them for the balance of $80,000.

Additional Advantages:
Cyber Liability and Data Security+ policyholders have access to a Breach Coach and a Security Coach. Claims reporting is available 24 hours a day, 7 days a week.

This document does not amend, extend or alter the coverage afforded by the policy. For a complete understanding of any insurance you purchase, you must first read your policy, declaration page and any endorsements and discuss them with your agent. A sample policy is available from your agent. Your actual policy conditions may be amended by endorsement or affected by state laws.

Coverage Part B

- **Data Breach Expense:** A retail drug store chain is hit with a data breach exposing the credit and debit card numbers and expiration dates for many of it's customers. State law requires the chain to report the breach and notify customers. The chain spends over $400,000 to hire a firm to conduct forensics to determine all those affected, re-secure its network, send out notification letters across multiple states and set up credit monitoring for the customers. In addition, $75,000 is spent on hiring a public relations firm to manage the publicity surrounding the event.

- **Cyber Extortion Threat Expense:** Jerry, the president of an insurance agency, arrives at work to find that he and his employees are locked out of the computer system. A hacker notifies him that they have 24 hours to pay $10,000 or all of the files on the server will be deleted. As the deadline nears, Jerry realizes that he cannot thwart this attack and is forced to pay the amount demanded.

Coverage Part C

- **Website Liability:** A coffee shop with a cinematic theme posts links on their website to movie coming attractions and uses images from movies in ads on their website. However, the coffee shop never received permission to post these images. Several movie studios threaten lto file suit for violations of intellectual property. At first, the coffee shop fights but then relents, agreeing to take down the postings after spending $10,000 in defense costs.

- **Website Liability:** Mike owns a boutique hotel along the Florida coast. The hotel has a website that includes a section for customer feedback. Mike monitors posts daily and is shocked to find a one star review from a well-known hotel reviewer who stated that his room and the property in general was dirty and that the hotel had poor customer service. Mike posted a reply on the blog that he remembered the reviewer, and he was the one who was unkempt, rude and confrontational with staff. The reviewer sued for $1,000,000 for libel and intentional infliction of emotional distress.

Coverage Part D

- **Identity Theft:** Carl is a small business owner of a local pizzeria looking to expand his operation. When Carl inquired about a loan to open up a new location, the bank turned him down due to poor credit. Apparently his identity was stolen, and the thief had opened up additional lines of credit and was purchasing big ticket items, such as a car and boat. They all went unpaid and collection attempts went to a fake address set up by the thief. Carl's operation is now headed toward bankruptcy as he cannot dedicate time to his business while he tries to clear his credit record, nor can he access credit to keep the business going.

This document does not amend, extend or alter the coverage afforded by the policy. For a complete understanding of any insurance you purchase, you must first read your policy, declaration page and any endorsements and discuss them with your agent. A sample policy is available from your agent. Your actual policy conditions may be amended by endorsement or affected by state laws.

Cyber Liability & Data Security+

Did you know?

- A study by a major credit card company found that 85 percent of all data breaches occur at the small business level
- Organized crime considers small businesses to be low risk, high reward targets
- Small business owners are popular targets of identity thieves because they have larger lines of credit, higher volume of transactions and valuable computer networks
- Common reasons personal information is breached include criminal hacking, lost or stolen laptops, computers or paper reports and negligent or malicious employee activity
- It is illegal for business owners to not report and not send notification to those whose legally protected personal information is breached

What are the costs of data breaches?

- Claims for failure to protect information, expense of legally required notifications and credit monitoring to those whose information is exposed, forensic expense to find out and resolve what happened, public relations expense to maintain business reputation, regulatory and Payment Card Industry (PCI) fines and hacker extortion demands
- In 2011, the average cost to business owners per record compromised was $194
- Small business owners have gone out of business due to identity thieves impersonating their business and personal name leading to loan defaults, inability to access credit and loss of business reputation

USLI can help protect you with the following product features:

COVERAGE FEATURES	USLI	COMPETITORS
Separate aggregate limits of liability per coverage part with option to combine into one aggregate limit		
Liability arising from both data breach and security breach		
Data breach expense and identity theft expense paid as incurred (pay-on-behalf) instead of by reimbursement		
Defense of regulatory proceedings		
Payment Card Industry (PCI) fines and penalties		
Data breach expense coverage including notification letters, public relations, forensics and credit monitoring		
Cyber extortion expenses		
Website liability including libel, slander, misappropriation of ideas, plagiarism, piracy, copyright and trademark violations		
Identity theft expense including credit monitoring and expense to retain specialists to resolve identity theft for board members and owners		
Access to the Business Resource Center which provides free and discounted business solutions to USLI policyholders		

This document does not amend, extend or alter the coverage afforded by the policy. For a complete understanding of any insurance you purchase, you must first read your policy, declaration page and any endorsements and discuss them with your agent. A sample policy is available from your agent. Your actual policy conditions may be amended by endorsement or affected by state laws.