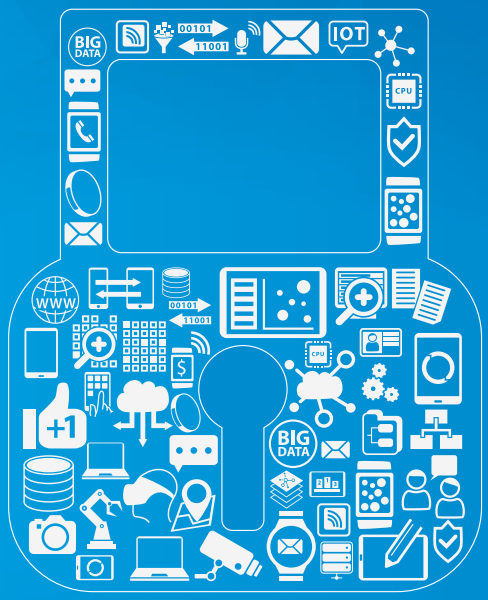
Bizlock Cyber Program
Effective July, 2024



BIZLOCK

Does your small business collect, use and/or disclose personal information? Do you operate a website? If so, it is entirely appropriate to have insurance to defend and cover the specialty cyber, privacy and information related liability exposures that exist. When it comes to cyber risks, our primary message is “Do your best, and insure the rest”. We understand that protecting computers and information against loss or theft is difficult. Because cyber risks will always remain, no matter how diligent your defenses, insurance presents a cost effective vehicle to transfer risk. We believe that cyber liability insurance is a fundamental need of every business, especially in today’s risk environment.

Bizlock Cyber Insurance Coverage Overview

Features	Core Cyber	Cyber Pro
Security & Privacy Liability Duty to defend coverage for third party claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.	√	√
Multimedia Liability Duty to defend coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.	√	√
Privacy Regulatory Defense and Penalties Duty to defend coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by a federal, state, local or foreign government agency.	√	√
PCI DSS Liability Duty to defend coverage for assessments, fines or penalties imposed by banks or credit card companies due to noncompliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.	√	√
Breach Event Costs Coverage for reasonable and necessary mitigation costs and expenses incurred because of a privacy breach, security breach or adverse media report, including legal expenses, proactive and reactive public relations expenses, advertising and IT forensic expenses, breach notification costs (including voluntary notification costs), and the cost to set up call centers and provide credit monitoring and identity theft assistance.	√	√
System Failure Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and business income loss and interruption expenses incurred, due to an unplanned outage, interruption, failure, suspension, or degradation of service of an insured computer system, including any such incident caused by a hacking attack.	√	√
Cyber Extortion Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.	√	√
Employee Personal Identity Protection Automatic identity protection includes VRS Elite Unlimited fraud victim resolution services combined with $15,000 identity insurance. No enrollment necessary.	√	√
Cyber Crime I. Financial Fraud – Coverage for loss of money or securities incurred due to financial fraud, including wire transfer fraud. II. Telecommunications and Utilities Fraud – i) Coverage for charges incurred for unauthorized calls resulting from fraudulent use of an insured telephone system and ii) loss resulting from the fraudulent use of utilities, such as electricity, water, internet access and cloud computing. III. Phishing Attacks (a) Your Phishing Fraud Loss – coverage for your loss of money, securities, or other property due to phishing schemes that trick an Insured to transfer, pay or deliver money, securities or other property to an unintended third party, plus expenses incurred to notify your clients or customers of such phishing fraud. (b) Client Phishing Fraud Loss – coverage for your loss of money, securities or other property which your client, customer or vendor intended to pay to you, but which was paid to an unintended third party due to a phishing scheme that tricked your client, customer or vendor by impersonating an Insured, plus the cost of reimbursing your customers, clients or vendors for their own losses that result from such phishing schemes.	Optional	√

Bizlock Cyber Insurance Coverage Overview Continued

Features	Core Cyber	Cyber Pro
Bodily Injury Liability Duty to defend coverage for third party claims alleging liability for bodily injury caused by a security breach or privacy breach.	X	√
Property Damage Liability Duty to defend coverage for third party claims alleging liability for property damage caused by a security breach or privacy breach.	X	√
TCPA Defense Defense-only coverage for claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.	X	√
Post Breach Remediation Costs Coverage for post-breach remediation costs incurred to mitigate the potential of a future security breach or privacy breach.	X	√
BrandGuard® Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach. A 2-week waiting period and 6-month period of indemnity apply to BrandGuard® coverage.	X	√
Dependent System Failure Coverage for (1) reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen and (2) business income loss and extra expenses incurred due to an unplanned outage, interruption, failure, suspension, or degradation of service of an IT service provider computer system that is caused by specified cyber perils, including a denial of service attack, malicious code, and acts of cyber terrorism. A 12-hour waiting period and 4-month period of indemnity apply to the business interruption coverage component of Dependent System Failure.	X	√
Bricking Loss Coverage for costs to replace computer hardware or electronic equipment that has been rendered nonfunctional due to a hacking attack, up to 125% of replacement value.	X	√
Property Damage Loss Coverage for damage to your property resulting from a hacking attack.	X	√
Reward Expenses Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, phishing attack or phishing fraud.	X	√
Court Attendance Costs Coverage for reasonable costs incurred to attend court, arbitration, mediation, or other legal proceedings or hearings as a witness in a third party claim covered under the policy.	X	√

This document provides summary information only. Insurance coverage is subject to specific terms, limitations and exclusions, and may not be available in all states. The above items are provided pursuant to our customer agreement.

Bizlock Insurance Services
CA License: 0D40585

BIZLOCK

Frequently Asked Questions

What is privacy and cyber risk?

Every business has data that can be damaged, lost or stolen. Computer systems and networks can also be attacked and damaged/destroyed. Data and cyber risks arise from the use of computer systems and the collection, use and storage of data, both electronically and on paper. Accidents and malicious attacks involving systems and the data can be devastating to a business. And, with proprietary and/or personal data being such a valuable asset, criminal attacks have become commonplace in businesses of all sizes, large and small.

What are some examples of the risks faced by small businesses?

Risks and exposures exist wherever information is collected. Sensitive, personally identifiable information (PII) of customers on computer systems, laptops, smart phones, external (thumb) drives, cloud data providers and paper office files all contain data that is very valuable to ID thieves and hackers. It's also susceptible to loss through negligence or accidents. Similarly, data in transit via email, web browsers and even the postal service is exposed. Data held by vendors, independent contractors or work-from-home employees are also big exposures. Data breach incidents can occur as a result of negligence of trusted employees, the lack of proper data security, and malicious hacking from ID thieves or rogue employees.

Regardless of how data is lost or destroyed, the current legal, regulatory and contractual landscape presents significant risks to every organization that loses data that is within its care, custody and control.

How can an organization best address the risks?

Information security best practices and ID Fraud risk management is essential to identify and minimize risks. Employee / management education, heightened security policies, procedures, and technology defenses are all important, as well network security. However, no organization can ever be 100% secure from fraud, which makes Cyber Liability insurance the vital last layer of security, i.e. the final safety net, when all other security measures have failed.

What is Cyber Liability Insurance?

Cyber liability insurance provides financial protection for data and electronic risks. Computer systems can be damaged and destroyed, and data can be lost, stolen and compromised. However, unlike other physical exposures, data is not tangible. This intangible exposure, which is not covered by traditional insurance coverage, gave rise to the first "cyber" or data risk insurance policies that date back to the mid1990's.

Isn't this covered by a General Liability policy?

No, not unless specifically endorsed. Traditional general liability policies (ISO policy forms) are now specifically excluding cyber risks as the intent was never to cover the exposures.

Do small businesses really have an exposure? What happens if they have a data breach without this coverage?

The exposure is definite, even with encrypted systems and devices. Not even the most secure, large and sophisticated organizations (e.g. Home Depot, Target or Chase Bank) can prevent losses from occurring. When it comes to measuring financial and/or reputational risk, the Ponemon Institute data breach studies suggest financial losses to businesses are roughly $200 per lost record.

Cyber Glossary

Business Interruption Loss

A business interruption loss can happen when a cyber-event causes a disruption in the operations of a company, which results in lost business revenue. Some of the more common cyber-attacks against businesses which may lead to a BI Loss include denial-of-service, insertion of malware or malicious code, and ransomware.

Business Interruption Waiting Period

The BI waiting period is a time-based deductible or retention. Any loss calculation amounts only begin to accrue following the established waiting period as provided in the policy declarations.

California Consumer Privacy Act (CCPA)

The CCPA is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds: (1) Has annual gross revenues in excess of $25 million; (2) Buys or sells the personal information of 50,000 or more consumers or households; or (3) Earns more than half of its annual revenue from selling consumers' personal information. Organizations are required to "implement and maintain reasonable security procedures and practices" in protecting consumer data.

Cyber Extortion

While similar to Ransomware, Cyber Extortion is a broader term in that it isn't limited to just malicious software which takes control of a system, but to any cyber event which the criminal seeks money in return for the promise of releasing sensitive information. This includes malicious software (Ransomware).

Dependent Business Interruption

In the interconnected global economy, a company's business may rely on the operations and products/services of another company (think of an Auto Manufacturer relying on the supply of steel to produce vehicles, or an online retailer relying on the functionality and dependability of a 3rd parties hosting platform). Dependent Business Interruption loss, also known as Contingent Business Interruption loss occurs as the insured is unable to access the necessary materials or services which support the insured's operations (raw materials, website functionality, cloud service provider, etc.), thus impacting revenues.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information. To fulfill the requirement for safeguarding sensitive information, the Department of Health and Human Services (HHS) publishes what is known as the HIPAA Privacy Rule. The Privacy Rule establishes national standards for the protection of certain health information, Protected Health Information (PHI).

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) contains within it, the HIPAA Security Rule. This rule establishes a set of national standards for the confidentiality, integrity, and availability of Protected Health Information (PHI). The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing the Security Rule, and it may conduct investigations and compliance reviews and administer penalties for companies found to be noncompliant.

Cyber Glossary – Continued

Multimedia Risk

This is a risk faced by many companies who create or disseminate information either electronically or physically. Risk is usually driven through the following areas: defamation, libel/slander, invasion of privacy, infringement of copyright and trademark, and plagiarism.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

PCI Fines and Penalties

A company (merchant) which accepts credit cards and has signed a Merchant Services Agreement (MSA) with their bank has an obligation to safeguard payment card data. If such merchant experiences a security breach involving payment card (PCI) data and is found to be non-compliant with PCI rules, they may be subject to PCI-DSS Fines and PCI-DSS Assessments and are required to indemnify their bank for costs incurred.

Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication, usually through email. Phishing attacks are usually not personalized to the victims but are usually sent to masses of people at the same time in order to increase the chance of success. Easily confused with "Spear-Phishing", which is a targeted or "spear" attack, phishing attacks are broader in nature.

Ransomware

Ransomware, one of the fastest-growing areas of cybercrime, refers to malicious software that is specifically designed to take control of a computer system or its data and hold it hostage so the attackers can demand payment from their victims.

Social Engineering

Also known as Fraudulent Wire Transfer Loss, a social engineering scheme is accomplished by tricking an employee of a company into transferring funds to a fraudster.

The fraudster sends an email impersonating a vendor, client, or supervisor of the company and advises that banking information for the vendor/client has changed or company funds immediately need to be wired at the "supervisor's" direction. The email looks authentic because it has the right logos and company information, and only careful study of the email will reveal that the funds are being sent to the fraudster's account. Unsuspecting and trusting employees unwittingly have cost their companies millions of dollars in connection with social engineering claims.

Spear Phishing

Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online. The attacker then disguises themselves as someone 'trustworthy' in an attempt to acquire sensitive information. Spear-phishing is the most successful form of acquiring sensitive information online.