

Cyber Liability Insurance

What does it cover?

Table of Contents

- What is Cyber Liability?
- Cyber Policy Coverages
- How Will a Policy Respond?

What is Cyber Liability?



Cyber liability insurance is an insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cyber security issues.



While each cyber policy is different, this presentation is meant to show you the types of coverage options that can be available.



Please review your individual cyber quote and/or policy to confirm what coverages you may or may not have.



Cyber Coverages

- First Party – Coverages & Services
 - Data Compromise Response Expenses
 - Computer Attack
 - Cyber Extortion
 - Misdirected Payment Fraud
 - Computer Fraud
 - Identity Recovery
 - Business Interruption & Business Interruption from Suppliers
 - Reputational Harm



Cyber Coverages Continued

- Third Party Coverages
 - Privacy and Network Security Liability
 - Electronic Media Liability
 - Regulatory Fines and Penalties
- Crime
 - Fraudulent Instruction (aka Social Engineering)
 - Funds Transfer Fraud
 - Telephone Fraud



First Party Coverages

Coverage: Data Compromise Response Expenses

Provides services to you if you experience a breach of personally identifying information (PII). PII includes SSN's, Drivers License #'s, Dates of Birth, Medical Info and Other Private Info. Services provided to you in the event of a breach include the following:

- 1) Forensic & Legal Assistance
- 2) Notification to persons who must be notified.
- 3) Credit monitoring and fraud protection services
- 4) Regulatory Fines and Penalties
- 5) Public relations expenses and crisis management consultants

Claim Example

You've gone paperless! You instruct your assistant to scan all documents into the computer and dispose of the hard copy files. They do a great job getting everything scanned in and they throw the hard copy files into the dumpster outback. Someone is dumpster diving and finds the old files and uses them to steal the PII of your clients and sell it on the dark web.



Claim Example 2

You're on a business trip and flying from Boston to Chicago. You set your laptop bag down on the floor at Starbucks while you grab a coffee to wait for your flight. When your coffee is ready you head to your gate, completely forgetting your bag. By the time you realize and go back to get it, it is gone, along with any PII located on it.



Coverage: Computer Attack

A computer attack that damages your data and systems. Coverage components include:

- Data Restoration
- Data Recreation
- System Restoration
- Loss of Business
- Extended Income Recovery
- Public Relations

Claim Example

You suffer a virus infection which corrupts data and causes computer systems to stop functioning.



Coverage: Cyber Extortion

Indemnifies you for cyber extortion threats, including ransomware and denial of service attacks. Coverage includes both the cost to investigate as well as approved extortion payments.



Claim Example

A ransomware virus infiltrates one of your business laptops. A demand is made for a Bitcoin payment to return your electronic credentials to you.





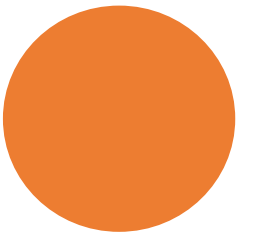
Coverage: Misdirected Payment Fraud

This is the intentional and criminal deception of you or your financial institution caused by a wrongful transfer event, that results in a direct financial loss to you.



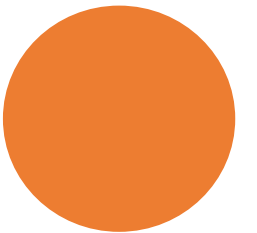
Claim Example

The CEO of a business is tricked into providing his account username and password to a bad actor. The bad actor then drains the bank account of funds.



Claim Example 2

A bad actor pretends to be the CEO and contacts an employee to make a funds transfer. The employee does as instructed and wires funds to the bad actor's bank.



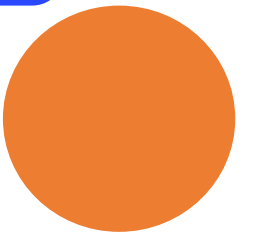
Coverage: Computer Fraud

This is the change of data or instructions within a computer system that results in a financial loss.



Claim Example

A bad actor infiltrates your company's computer system and changes the banking instructions. With the change, they were able to divert your payroll funds into their account.



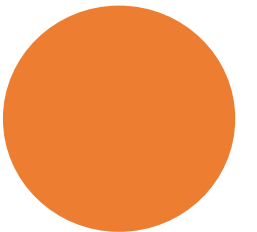
Coverage: Identity Recovery

If someone has their identity stolen due to a cyber breach, the policy will respond to assist them with this.




Claim Example

You are sued due to unauthorized credit card accounts being opened for one of your clients whose information was stolen from your computer system. The bad actor used the new accounts to make fraudulent credit card purchases.





Coverage: Business Interruption & Business Interruption from Suppliers

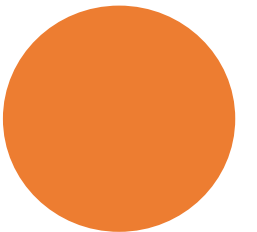
- Business Interruption: Income loss and expenses incurred during the interruption or slowdown of operations caused by a cyber event at your business.
 - Business Interruption from Suppliers: Income loss and expenses suffered by your business due to a vendor or supplier experiencing a cyber vendor of their own.
- 

Claim Example



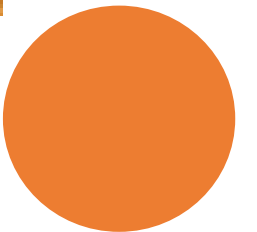
Your business conducts 100% of its sales online. One day, your business suffers a cyber attack which leaves your website down for nearly 2 weeks, during which time you could not sell any product.

SORRY
WE ARE
CLOSED



Claim Example

Your business bakes and sells spiced cookies which require a very select group of spices that are hard to source. You have been lucky and found a supplier that can provide these for you. The spice company suffers a cyber attack and as a result it cannot deliver its spices to you, thus, you are unable to bake and sell cookies during this time.





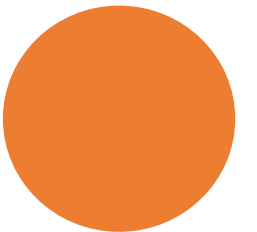
Coverage: Reputational Harm

Income loss incurred due to a cyber event becoming public and hurting your reputation.



Claim Example

Your company suffers a data breach that affects a lot of your clients. While you try and keep the incident quiet, the local news hears of the event and makes a top story about it. You notice that you are no longer getting any new clients as your company name is now associated with a large cyber event and clients are leery to work with you.






Third Party Coverages



Coverage: Privacy & Network Security Liability

Coverage for damages and expenses for a claim arising out of:

- 1) Data breach
 - 2) Security breach
 - 3) Failure to report a data or security breach
 - 4) Failure to comply with your own privacy policy
- 

Claim Example

A financial institution is the target of a cyber attack and suffers unauthorized third-party access into a portion of their processing system. As a result, certain customers information is stolen, including names, social security numbers, account and pin numbers. A customer who is one of those affected then sues the financial institution for failure to adopt or maintain reasonable procedures and adequately secure its servers and computer storage systems.



Coverage: Electronic Media Liability

Coverage for damages and expenses for one or more of the following acts during your display of media material on your website or social media pages:

- 1) Defamation, libel, slander or other tort related disparagement
- 2) Violation of rights of privacy of an individual
- 3) Invasion or interference with an individuals right to publicity
- 4) Plagiarism, piracy, misappropriation of ideas
- 5) Infringement of copyright
- 6) Infringement of domain name, trademark, trade name, logo, etc.

Claim Example


You are a huge Justin Bieber fan. While he has never tried your product, you are confident that if he did, he would love it! You use Justin Bieber's photo on your website without his permission. You get a letter demanding it be removed and also a demand for monetary damages.





Coverage: Regulatory Fines and Penalties

Provides coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred because of privacy regulatory proceedings or investigations brought against you by federal, state or local governmental agencies.



Claim Example

A restaurant discovers malware operating on their point-of-sale (POS) system. The malware is designed to access payment card data, including customer names and card numbers used on the POS system. The restaurant discloses the breach in a press release, and a customer affected by the breach subsequently files a consumer complaint with the Federal Trade Commission (FTC). The FTC investigates and finds that a lack of technical safeguards contributed to the theft of the credit card data. The FTC orders the restaurant to pay civil fines and penalties for unfair data security practices.





Crime Coverages



Coverage: Fraudulent Instruction (AKA Social Engineering)

Indemnifies you for direct financial loss sustained from fraudulent instruction provided by a person purporting to be a vendor, client or authorized employee that is intended to mislead you through misrepresentation of material fact.



Claim Example

You receive an email from a vendor you work with asking you to cancel the check you just mailed to them, and instead wire the money to their bank account. You wire the money to them, before realizing the email you reacted to was a spoofed email address.





Coverage: Funds Transfer Fraud

A fraudulent instruction that is electronically sent to a financial institution that directs the transfer, payment or delivery of money or securities from your account.



Claim Example

A hacker is able to find your bank information and directs your bank to wire your money from your account into their own account.





Coverage: Telephone Fraud

Indemnifies you for direct financial loss resulting from a third-party gaining access to and using your telephone system.



Claim Example

A hacker gains access to your company's phone line and using their equipment and programs, makes thousands of phone calls to international long-distance numbers or to phone number that charge callers per minute (e.g. psychic hotlines).



You bought the cyber policy – and now you have a claim – so How Will Your Policy Respond?

There are many ways your policy responds to assist you after a loss, including but not limited to:

-Forensic IT Review – what went wrong?

Legal Review – any there any fines levied? Notifications required?

Notification expenses.

Services to affected individuals.

Regulatory fines and penalties.

PCI Fines and Penalties.

Public relations/crisis management.

Data and system restoration/recreation.

Loss of Business.

Cost of an investigator (if needed).

Approved extortion payments.

Costs of defense, settlement and judgement.



In Summary

- Regardless of your company's size or your industry, The Richards Group has the right carriers to ensure your business is protected from Cyber Liability.
- Let us discuss with you your specific needs and find the right Cyber Liability program for you.
- If you are looking for resources to increase your IT Security, we have partnered with a local IT firm that can help ensure you are using best practices to protect your business as well.